DEFENSE MANPOWER DATA CENTER

INFORMATION ASSURANCE PROGRAM

INFORMATION ASSURANCE POLICY

4 November 2009

Version 2.9.6

TABLE OF CONTENTS

APPENDICES

INFORMATION SYSTEMS SECURITY POLICY

1. OVERVIEW

1.1 Purpose

With this policy, Defense Manpower Data Center (DMDC) management establishes information security as one of our top priorities. DMDC is the steward for DOD manpower resource information and is charged with delivering critical services to users of that data. DMDC management is committed to safeguarding our information assets while guaranteeing that data and services are available to authorized users and not available to unauthorized users.

The goal of this policy is to lay out the rules by which people given access to DMDC technology and information assets must abide. It also provides a baseline from which to acquire, configure, and audit computer systems and networks for compliance with the policy.

All managers, staff, and users are required to protect DMDC technology and information assets. Failure to do so, and more specifically, failure to adhere to these security policies will result in disciplinary action and possibly even termination. If criminal laws are violated, DMDC will notify the appropriate authorities and cooperate in prosecution.

1.2 Scope

This policy applies to all employees, contractors, military, consultants, temporaries, and other workers at DMDC, including those workers affiliated with third parties who access DMDC computer networks. The policy also applies to all computer and data communication systems owned by and/or administered by DMDC or operated on behalf of DMDC.

1.3 Information Assurance Program Management and Administration

The Information Assurance (IA) program is administered by DMDC Information Systems Security Group (DISSG).

All DMDC associates – managers, employees, military, contractors, and affiliates – are part of the security solution and have a responsibility for securing our information resources.

1.3.1 Director

The ultimate authority and responsibility for security at DMDC rests with the Director. The Director is the Designated Approving Authority (DAA), determining whether security controls in DMDC Information Systems (IS) are acceptable and authorizing their operation.

1.3.2 Chief Information Officer

The Chief Information Officer (CIO) is responsible for strategic planning of information technology and ensuring that security is an integral component of all existing and proposed systems.

1.3.3 Information Assurance Manager

The Information Assurance Manager (IAM) for DMDC reports to the CIO. The IAM is responsible for the Information Assurance (IA) program and has the authority and responsibility to ensure that the requirements established in DODI 8500.2 are satisfied.

1.3.4 DMDC Information Systems Security Group

DISSG is the branch of the CIO office that is responsible for IS security in the enterprise. DISSG develops security policy in conjunction with senior management, and manages the Certification and Accreditation (C&A) process on behalf of the Director.

1.3.5 Information Assurance Officer

For each IS, the IAM designates the Information Assurance Officer (IAO). The IAO is a member of the C&A team. The IAO administers security compliance monitoring and reporting and is the liaison to the IAM through DISSG.

1.3.6 Division Chiefs and Managers

DMDC managers are responsible for ensuring that all acquired or developed IS include appropriate security mechanisms and can be operated in a secure manner. Managers are required to plan and budget for security in projects under their control. Managers must ensure that all subordinates are aware of security requirements and receive security training appropriate for their roles.

1.3.7 Developers

Developers must ensure that security requirements are incorporated into their design. All software activities must be carried out in a disciplined manner observing appropriate coding standards, guidelines, and DMDC policy.

1.3.8 Systems and Technical Support Division

Systems and Technical Support (STS) Division personnel control IS that may affect many users. They therefore need a deeper understanding of security issues and must receive additional security training besides the required annual security awareness training. Personnel with administrator-level access are held to a higher standard.

1.3.9 Users

Security is everyone’s responsibility. All users must comply with this policy.

1.4 Requests for Exception to Policy

All requests for exceptions to security policies or procedures must be made in writing to DISSG. Requests must provide adequate alternatives that provide equivalent protection for all affected personnel, property, or facilities. Requests should be for a specified period of time and should include a plan to bring the excepted IS into compliance with policy or explain why compliance isn't feasible.

1.5 Effect on Other Policies

This policy supersedes all others governing security administration at DMDC. This policy implements and extends Federal and DOD requirements. This policy may increase, but in no case decrease, a Federal or DOD requirement.

2. ENTERPRISE SECURITY POLICY

2.1 Physical and Environmental Security

DMDC is a controlled access facility. All persons inside the facility must provide positive identity confirmation to be issued identification (ID) badges, whether temporary or permanent. Visitors without identity verification will not be issued ID badges and must be escorted at all times.

All access and exit will be recorded and identify the specific individual. Sensitive areas within the facility will have further controls to limit access to specifically authorized individuals.

Appropriate environmental safeguards will be maintained to ensure the safety and protection of personnel and assets.

2.2 Personnel Security Policy

All personnel, whether military, civilian, or contractor must successfully complete security investigations appropriate to their roles. Upon termination of services, all personnel must be out-processed through standard procedures that include return of equipment, termination of access, and debriefing.

2.3 General Usage Policy

General DMDC IT resources are provided and managed by STS. Equipment assigned to you is DOD equipment and should be used for authorized purposes only. Any activity may be monitored and is subject to audit. You are responsible for protecting network credentials issued to you and for all activity using them. You are also responsible for appropriate protection of the information you use or generate.

Only government-owned or government-managed equipment should be used for DOD activities.

It is understood that on occasion incidental personal use may occur provided it violates no laws, causes no disruption, and is within the scope of DMDC's appropriate use policy.

2.4 Computer and Operations Management

General computing resources, including infrastructure, servers, desktops, and notebooks will be managed by STS. Equipment will be secured and configured in conformance with all Federal and DOD requirements.

2.5 Audit and Compliance

All DMDC IS must include sufficient means to reconstruct or review system and user system activities related to operations, procedures, or events occurring on the DMDC network and systems.

Audit data will be collected and stored in accordance with all Federal and DOD requirements. This includes periodic review of security-related logs.

2.6 Asset Classification and Control

Positive asset control procedures must be in place throughout the life-cycle of IT equipment. All information assets of a sensitive nature should be appropriately labeled and controlled.

2.7 Business Continuity Planning

Business continuity must be considered in the design and operation of all critical systems.

2.8 Account Management

All persons granted access to DMDC resources are responsible for the safeguarding of their network credentials. Account use is audited and individuals are responsible for all actions occurring using their credentials. Access to specific systems or applications is only granted to persons needing it to support specific work.

Network accounts will only be enabled for users that have:

1) been vetted at the appropriate level for their access as per DMDC SOP;
2) completed Security Awareness training;
3) completed Privacy Act training;
4) executed the DMDC Information Systems User Agreement.

2.9 Privacy Act and Other Sensitive Data

Privacy Act and other sensitive data entrusted to DMDC must remain protected at all times. This includes receiving and sending of that data, as well as when that data is at rest on a storage device and any other time the data is removed from the workplace to accomplish authorized work.

Privacy Act data and other sensitive data must not be stored on personal IT devices. All persons with access to Privacy Act data must be vetted as ADP-II or higher.

DMDC will provide access to non-public data, i.e. sensitive and proprietary data, to persons or organizations who: 1) have a legitimate Need-To-Know (NTK), as determined by DMDC; 2) have the proper vetting level or clearance for the specific information; and 3) have procedures and information security measures in place to assure the confidentiality and integrity of the information.

Non-public data must only be exchanged in a secure manner. When transmitted electronically, including via email, non-public data must be encrypted.

Violations of this policy may result in disciplinary action.

2.10 Information Technology Acquisition

All IT acquisition, either hardware or software, must comply with Federal and DOD requirements and be coordinated through DMDC management, the Developers Steering Group (DSG), the Integrated Development Group (IDG), the Technical Review Board (TRB), and DISSG.

2.11 Wireless

All wireless use must conform to DOD current standards. Wireless operation must be coordinated with STS and DISSG. Periodic compliance audits will be conducted by DISSG.

2.12 Data Security

All data must be protected at a level commensurate with the threat environment. The level of protection will comply with DOD policy and standards.

2.13 Certification and Accreditation

All DMDC systems and applications must be accredited by the DAA and have an Authority to Operate (ATO), Interim Authority to Operate (IATO), or Interim Authority to Test (IATT) before being placed into production.

Systems must have security controls tested at least annually and be reaccredited every three years or whenever there is a major change to the system.

2.14 Access

Access to systems or information will only be granted to personnel who are cleared at the appropriate level and have a need-to-know.

2.15 Incident Response

All employees should be vigilant for security breaches. As soon as employees become aware of an incident, they should report it to their Supervisors and to DISSG. DISSG will manage, document, and log the investigation per the incident response process.

2.16 Security Awareness and Training

All users of DMDC resources must complete security awareness refresher training at least annually. New users will not be given access to DMDC systems until they complete security awareness training, Privacy Act Training, and execute a User Agreement.

2.17 Operational Security

Since an adversary can accumulate and correlate sensitive unclassified data from various sources to deduce useful and potentially damaging information, all users of DMDC resources need to be aware of the need for Operational Security (OPSEC).

OPSEC will be included in the annual Security Awareness and Training for all users.

2.18 Information Operations Condition (INFOCON)

DMDC will comply with requirements for security posture based on updated cyber threat and INFOCON status.

2.19 Portable Devices

The use of portable devices must conform to all DOD and DMDC security policies as well as device-specific policies. Portable devices include laptops, PDAs, cell phones, thumb drives/USB drives, MP3 players, camcorders, digital cameras or any other device with storage, connectivity, or data capture capability. USB devices such as MP3 players, camcorders, or digital cameras are not to be attached to IS without DAA approval.

In general, use of personally owned devices other than cell phones is not allowed except in the conference area. In no case is it permissible to connect a personally owned device, including thumb drives, to DMDC equipment or networks without explicit authorization. Furthermore, no IS shall have its BIOS set to allow a boot from any USB device.

POLICY 2.1 – Physical and Environmental Security

2.1 Policy Statement

DMDC is a controlled access facility. All persons inside the facility must provide positive identity confirmation to be issued identification (ID) badges, whether temporary or permanent. Visitors without identity verification will not be issued ID badges and must be escorted at all times.

All access and exit will be recorded and identify the specific individual. Sensitive areas within the facility will have further controls to limit access to specifically authorized individuals.

Appropriate environmental safeguards will be maintained to ensure the safety and protection of personnel and assets.

POLICY 2.2 – Personnel Security

2.2 Policy Statement

All personnel, whether military, civilian, or contractor must successfully complete security investigations appropriate to their roles. Upon termination of services, all personnel must be out-processed through standard procedures that include return of equipment, termination of access, and debriefing.

2.2.1 Scope

This policy applies to all DMDC associates, whether Government or contractor.

2.2.2 Rationale

To minimize risk, all associates must be vetted at a level appropriate to their roles before being granted access to information assets. Likewise, when an associate's role is terminated, access must no longer be granted.

2.2.3 Policy Implementation

All associates must be vetted including background checks before being granted a network account.

When terminated, the associate's access privileges must also be terminated and the associate's supervisor should use the Associate Termination Checklist to out-process the Associate.

2.2.3.1 Personnel Commencement

When new associates are hired, certain actions must be completed before they commence their assigned roles. These actions vary depending on whether the associate is a government employee or a contractor and depending on the level of trust associated with the role.

2.2.3.1.1 Government Employees

Background investigations for military and civilian employees are conducted by the appropriate agency in accordance with DOD 5200.2-R, Personnel Security Program.

2.2.3.1.2 IT and Other Special Vetting

Employees whose job functions include the operations, maintenance, administration, or development of IT will be assigned a job category of IT-I, IT-II or IT-III depending on their specific roles and will be vetted accordingly as specified in DOD 5200.2-R.

Persons with access to Privacy Act protected data will be vetted minimally at the IT-II level and may be vetted higher depending on the nature of the data and job functions.

2.2.3.1.3 Contractor Vetting

PURPOSE. This SOP provides procedures, responsibilities, and guidance for implementing the DMDC Personnel Security Program for contractors and consultants.

APPLICABILITY. This SOP applies to all DMDC contractors and consultants with direct or indirect access to DMDC systems or data. This includes those who bill DMDC for goods or services or that are assigned or working on the DMDC account at any remote sites.

POINT OF CONTACT. The point of contact for this SOP is the DISSG Personnel Security Office as listed at:

http://wwwi/iweb/common/dissgwebsite/htm/Team/team.htm.

RESPONSIBILITIES. DISSG holds the primary responsibility for management and execution of contractor or consultant personnel security trustworthiness determinations throughout DMDC.

1. The DMDC Information Systems Security Group (DISSG) will:
    a. Develop personnel security policies, procedures, and guidance;
    b. Manage administrative tasks associated with personnel security;
    c. Ensure that each contractor completes the Standard Form 85P (SF 85P), FD 258 (fingerprint card), DLAH Form 1728, and signs the Information Systems User Agreement in a timely manner;
    d. Obtain an appropriate ADP level requirement from the DMDC Division Chief via the DMDC Form 85R;
    e. Forward the contractor or consultant process application to the appropriate investigative agency;
    f. Monitor, administer, and oversee a timely vetting process for contractor or consultant applications;
    g. Maintain contractor and consultant security files;
    h. Audit the process as necessary at the discretion of the Information Assurance Manager (IAM).
2. The Director may authorize the use of foreign nationals when deemed necessary by authorizing on the DMDC Form 85R and forwarding to DISSG.
3. Division Chiefs will assign vetting levels for all contractors in their division and authorize the hiring or consulting of US citizens by signing the DMDC Form 85R and forwarding to DISSG.

4. Contract Managers or designees will:
    a. Use DMDC Form 85R to:
        i. Notify DISSG of new hires and consultants;
        ii. Declare transfers, terminations, or change in vetting level for current contractors;
    b. Request Division Chief approval signature and vetting level designation for new hires, incoming consultants, and changes to vetting levels for current contractors;
    c. Forward new hires an electronic "Vetting Package Email" containing SF 85P and vetting instructions;
    d. Ensure each new hire prints a hard copy of SF 85P, which covers minimally the last seven years of employment and residency; this action is to be completed prior to or on the first day of employment;
    e. Ensure the DLAH Form 1728 is filled out as follows:
        i. Contractor shall fill out Part I, questions 1-8 and 16, parts a, b, c, d;
        ii. Contract Hiring Managers shall fill out Part I, questions 9-14;
    f. Ensure contactors show an original certified proof of U.S. citizenship to DISSG or a designee; if location makes the task impractical, refer to section "Contractors working off-site or at remote location";
    g. Ensure each contractor completes the following prior to or on the first day of work:
        i. Security Awareness training, and provide certificate of completion;
        ii. Privacy Act training, and provide certificate of completion;
        iii. Sign the DMDC IS User Agreement;
    h. Fill out and sign DMDC Form 85C Pre-Account Activation Checklist;
    i. Forward all completed forms to the DISSG office or designees.
5. Contractor will, before or on the first day of reporting to work:
    a. Complete and print the SF 85P covering the last seven years, including employment and residence;
    b. Complete one FD 258 fingerprint card with a designated security officer;
    c. Provide proof of U.S. citizenship, refer to section "Explanation of Forms and Documents";
    d. Complete the Security Awareness training and provide certificate;
    e. Complete Privacy Act training and provide certificate;

f. Sign the DMDC IS User Agreement.

SPECIAL CASES.

1. Contractor with active security clearance. Contractors that hold an active security clearance should use the following procedures:
    a. The contractor security office will forward an official Visit Authorization Request (VAR) to the DISSG Personnel Security Office.
    b. The contractor hiring manager will provide the following to the DISSG Personnel Security Office::
        i. Completed and approved DMDC Form 85R;
        ii. Completed DLAH Form 1728.
    c. The contractor is required to complete:
        i. Security Awareness training and provide certificate;
        ii. Privacy Act training and provide certificate;
        iii. Sign the DMDC IS User Agreement.
2. Consultant with active security clearance. If the contractor is a temporary consultant or subject matter expert sponsored by a primary contractor, the consultant must hold an active clearance at the level required by the Division Chief as specified on DMDC Form 85R.

    The manager or designee should accomplish the following to DISSG at least one week prior to visiting the DMDC facility:

    a. Securely provide the consultant's full name and Social Security Number (SSN) to DISSG;
    b. Provide approved DMDC Form 85R to DISSG.

    If the consultant will have direct or indirect access to a computer or sensitive data such as PII, the following must also be accomplished prior to account activation or access:

    a. Complete Security Awareness training and provide certificate;
    b. Complete Privacy Act training and provide certificate;
    c. Sign the DMDC IS User Agreement.

    For additional consultant information, refer to "Consultant Vetting Requirements" at:

    http://wwwi/iweb/common/dissgwebsite/docs/Personnel/Consultants_Requirements.pdf.

3. Contractor working off-site or at remote location. In outlying areas with no trusted government presence, contactors may do the following:
    a. Citizenship Verification. Submit a notarized copy of the original proof of citizenship document.
    b. FD-258 Fingerprint Card. Have fingerprints taken at local police department.
    c. Security Awareness and Privacy Act Training. Contact DISSG Personnel Security office to request a CD containing the training.

EXPLANATION OF FORMS AND DOCUMENTS. The Department of Defense conducts background investigations to establish that ADP applicants are eligible for the required trustworthiness determination. The background investigations shall be initiated prior to a contractor or consultant working on a DMDC ADP system or billing DMDC for services. In rare circumstances, exceptions to this policy may be granted. These will be addressed on a case-by-case basis by the IAM and DMDC senior managers.

1. DMDC Form 85R Contractor Vetting Status Form. Serves various functions for managing access to contractors and consultants. The functions are as follows:
    a. Proves that the Division Chief approves the visit or hiring. This is primary permission to work on the DMDC government system;
    b. Allows the Division Chief to specify the required level of access that the individual requires for the task at hand;
    c. Alerts the Director that a foreign national may be working on a DoD system.
2. SF 85P Questionnaire for Public Trust Positions.
    a. Contractors shall electronically complete and print the SF 85P covering the last seven years.
    b. Contractors are required to sign and date in black ink on page 7 and page 8 (*Certification that My Answers Are True* and *Authorization for Release of Information*).
    c. The original SF 85P should be delivered to DISSG.
3. FD-258 Fingerprint Cards.
    a. Fingerprints will be executed at DMDC East or DMDC West by designated security personnel;
    b. For those contractors who are located in remote locations and are unable to have their prints taken at DMDC, they may have their prints taken at their local police department. The executed FD 258 fingerprint card must be forwarded to DISSG.
4. DLAH Form 1728. Request for Information Technology Access.
    a. The contractor shall complete and sign Part I Questions 1-8 and 16 parts a, b, c, and d;
    b. The hiring manager shall fill out Part I, questions 9-14;
    c. The Privacy Act Data box should be checked.

5. Citizenship Verification. The only acceptable documents for proof of U.S. citizenship are the following:
    a. Birth Certificate (if born in the U.S.);
    b. State Department Form 740 (Report of Birth Abroad of a U.S. Citizen);
    c. U.S. Passport;
    d. Certificate of Naturalization.

    DISSG will make a copy of the document for inclusion into the vetting request application.
6. Visit Authorization Request (VAR). A Visit Authorization Request is an official request for access to a sensitive DMDC government system or location. It indicates the contractor clearance level. VARs may not exceed one year. The VAR must be signed by the contracting firm'' Security Officer. The contacting firm's security office must submit the VAR to DISSG Personnel Security Office.
7. Security Awareness Training. The Security Awareness training and the Privacy Act training are required to be taken onsite prior to account activation/initiating work on a DMDC system.
    a. West coast managers may enter appointments in the calendar <RSS DMDCE DISSG RM 4030>.
    b. East coast managers may enter appointments in the calendar <RSS DMDCE 1600W New Hire Training>.
    c. If access to the calendars is not available, contact the DISSG Personnel Security office to schedule an appointment.
    d. If the contractor or consultant is at a different DMDC location other than East or West, such as Auburn Hills, a copy of a CD with the training may be released to the new hire. Contact the DISSG Personnel Security Office to request a copy.
    e. Certificates of completion can be printed at the end of the training as proof that the requirement has been fulfilled.
8. Privacy Act Training. Refer to Section 7 above.
9. Information Systems User Agreement. Refer to Section 7 above.
10. DMDC Form 85C Pre-Account Activation Checklist. Contract managers or their designees shall fill out and sign the Pre-Account Activation Checklist. This form will ensure that all the requirements have been requested and submitted to DISSG.

2.2.3.2 Personnel Termination

For any termination, an Employee Action Form (EAF) should be submitted as soon as possible. Additionally, the Division Chief of Operations and the Division Chief of Systems should be explicitly notified to ensure there is no delay regarding termination of physical access and network access.

The *Associate Termination Checklist* should be used when employment for an individual, whether government or contractor, is terminated. All of the steps are necessary, however carrying them out in some cases may be problematical, e.g. in the case of an immediate dismissal for cause. Contractors may have additional actions to take that are specific to each contractor, e.g. return of corporate ID badges or termination of access to internal corporate systems.

Termination can be:

- Voluntary, as is the case for resignation or retirement;
- Involuntary-Foreseen, such as a reduction in force, or inadequate performance over a period of time; or
- Involuntary-Unforeseen, as for a serious breach of trust or duty.

The first two cases allow for preparation ahead of time, and, usually for Voluntary and even much of the Involuntary-Unforeseen, the individual remains cooperative and can be relied upon to facilitate the process.

For Involuntary-Unforeseen termination, additional steps need to be taken immediately and the completion of the remaining items on the checklist may become more difficult because of the associate's absence or non-cooperation.

Immediate Actions - Involuntary-Unforeseen Termination

The *Immediate Associate Termination Checklist* should be used when an individual is to be fired without warning, as in the case of a serious breach of duty or trust or criminal activity. The most immediate concern is to ensure the safety of personnel (including the departing individual), ensuring security, protecting the interests of the business, and preventing disruption of ongoing activities. The individual must be escorted from the site expeditiously. Nevertheless, it should be carried out in a professional and responsible manner.

Once the immediate actions from this checklist have been accomplished and normal operations secured, the standard *Associate Termination Checklist* should then be followed.

2.2.3.2.1 Immediate Associate Termination Checklist

Immediate Associate Termination Checklist	
[ ]	Notify Division Chiefs for Facilities, Systems, and CIO of impending action. When possible, this notification should occur prior to contacting the individual and must involve positive, acknowledged contact – not email or voicemail. If prior notification couldn't be made due to the nature of the situation, then notification should be made as soon as possible. A representative from each of the above organizations must be engaged in the termination process.
[ ]	Remain polite and respectful.
[ ]	Ensure the individual is not a danger to himself/herself or other personnel. (If he/she appears to be, help other personnel to safety and call law enforcement authorities and security personnel immediately.)
[ ]	Utilize internal security personnel.
[ ]	If individual's action is criminal, notify authorities.
[ ]	Remove individual to a private area, e.g. Supervisor's office.
[ ]	Notify Systems Division Chief (or delegate) to disable individual's network account immediately.
[ ]	State the offense calmly and with a witness in the room.
[ ]	Tell the individual his/her employment is terminated.
[ ]	Allow the individual to ask any questions about the end of employment.
[ ]	Collect CAC and any supplemental ID badges.
[ ]	Collect keys to office, desk, and file cabinets.
[ ]	Collect current contact information including forwarding address and emergency contact.
[ ]	If individual needs to retrieve personal items from work area (e.g., jacket, purse, car keys, etc.), provide escort.
[ ]	If necessary, provide individual with contact information to arrange a future time to pack and remove personal property from his/her work area.
[ ]	Escort the individual from the building.

2.2.3.2.2 Associate Termination Checklist

Associate Name (Last, First MI):		ID No.:	
Separation Date:		Division:	
Date Hired:		Separation Date:	
Note:			
The person who will receive access rights over the user's files and directories:	Name:		
	User ID:		

Associate Termination Checklist	
Physical Access	
[ ]	Collect CAC and any supplemental ID badges.
[ ]	Collect keys to office, desk, and file cabinets.
[ ]	Collect other keys. Specify:
Administrative	
[ ]	Submit Employee Action Form.
[ ]	Notify Systems Division and Operations Division explicitly.
[ ]	Collect current contact information including forwarding address and emergency contact.
[ ]	Update enterprise lists – telephone directory, offices, voicemail, email groups, organization chart, duty rosters, etc.
[ ]	Reassign any delegated authorities.
[ ]	Notify Security.
[ ]	Notify Vetting Officials.
[ ]	If authorized purchaser, COTR, or technical support POC, notify suppliers and vendors.
Financial	
[ ]	Collect purchasing credit cards.

[ ]	Collect telephone calling cards.
[ ]	Discontinue Government-provided offsite support contracts – e.g., DSL line.
Access Accounts and Codes	
[ ]	Disable network account.
[ ]	Disable machine and application specific accounts – Unix, mainframe, ftp, application-maintained accounts, etc.
[ ]	Change administrative passwords to which individual had access – Unix, Windows local administrator, network devices, etc.
[ ]	Change any entry codes known to the individual.
[ ]	If the associate has a security clearance, Security Officer needs to perform a security outbrief.
[ ]	If the associate had CLAB access, notify CLAB manager to update the CLAB access list.
Resources	
[ ]	Retrieve cell phone.
[ ]	Retrieve PDA.
[ ]	Retrieve laptop. Verify operational status by booting system.
[ ]	Retrieve pager.
[ ]	Retrieve peripherals – printer, scanner, removable drive, external burner, thumb drive, etc.
[ ]	Retrieve books, manuals, documentation, CBTs, special-purpose software and licenses.
[ ]	Ensure access to any encrypted files or emails.
Other	
[ ]	Execute any Contractor specific procedures.
[ ]	Retrieve off-site GFE (e.g., desktop computer).

POLICY 2.3 – General Usage Policy

2.3 Policy Statement

General DMDC IT resources are provided and managed by STS. Equipment assigned to you is DOD equipment and should be used for authorized purposes only. Any activity may be monitored and is subject to audit. You are responsible for protecting network credentials issued to you and for all activity using them. You are also responsible for appropriate protection of the information you use or generate.

Only government-owned or government-managed equipment should be used for DOD activities.

It is understood that on occasion incidental personal use may occur provided it violates no laws, causes no disruption, and is within the scope of DMDC's appropriate use policy.

2.3.1 Policy Implementation

When using a DOD computer system to process classified information, check the security accreditation level of this system. Do not process, store, or transmit information classified above the accreditation level of this system. This computer system, including all related equipment, networks, and network devices (includes Internet access) are provided only for authorized U.S. Government use.

DOD computer systems may be monitored for all lawful purposes, including ensuring their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security. Monitoring may include active attacks by authorized DOD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied, and used for authorized purposes. All information, including personal information, placed on or sent over this system may be monitored.

Use of any DOD system, authorized or unauthorized, constitutes consent to monitoring. Unauthorized use of any DOD computer system may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or other adverse action.

IS Use Policy

a. **Appropriate Use**. IS may only be used for their authorized purposes – that is, to support the functions and specific missions of DMDC. The particular purpose of any IS as well as the nature and scope of authorized, incidental personal use may vary according to the duties and responsibilities of the user.

Examples of acceptable use include, but are not limited to the following:

1) Accessing the Internet, computer resources, facsimile (fax) machines, and phones for information directly related to work assignments.

2) Off-hour usage of computer systems for school related work sanctioned by senior management.

3) Job-related On the Job Training (OJT).

b. **Proper Authorization**. Users are entitled to access only those elements of IS that are consistent with their authorization.

c. **Specific Proscriptions on Use**. The following categories of use are inappropriate and prohibited:

1) **Use that impedes, interferes with, impairs, or otherwise causes harm to the activities of others**. Users must not deny or interfere with or attempt to deny or interfere with service to other users in any way, including by "resource hogging," misusing mailing lists, propagating "chain letters" or virus hoaxes, "spamming" (spreading email or postings widely and without good purpose), or "bombing" (flooding an individual, group, or system with numerous or large email messages). Knowing or reckless distribution of unwanted mail or other unwanted messages is prohibited. Other behavior that may cause excessive network traffic or computing load is also prohibited.

2) **Religious or political lobbying.** Any use for religious or political lobbying, such as using Email to circulate solicitations or advertisements. Use of IS in a way that suggests DMDC endorsement of any political candidate or ballot initiative is also prohibited. Users must refrain from using IS for the purpose of lobbying that connotes organizational involvement.

3) **Harassing or threatening use**. This category includes, for example, display of offensive, sexual material in the workplace and repeated unwelcome contacts with another.

4) **Use that damages the integrity of DMDC or other IS**. This category includes, but is not limited to, the following activities:

a) **Attempts to defeat system security**. Users must not defeat or attempt to defeat any IS's security – for example, by "cracking" or guessing and applying the identification or password of another user, or compromising room locks or alarm systems. (This provision does not prohibit, however, DISSG or Systems Administrators from using security scan programs within the scope of their authority.)

b) **Unauthorized access or use**. The DMDC recognizes the importance of preserving the privacy of Users and data stored in IS. Users must honor this principle by neither seeking to obtain unauthorized access to IS, nor permitting nor assisting any others in doing the same. For example, a non-DMDC organization or individual may not use IS without specific authorization. Privately owned computers may not be 1) connected to the DMDC network infrastructure, 2) used to provide public information resources concerning the DMDC or, 3) used to process DMDC sensitive data, or 4) used to facilitate services to gain access to DMDC IS resources or information. Similarly, Users are prohibited from accessing or attempting to access data on IS that they are not authorized to access. Furthermore, Users must not make or attempt to make any deliberate, unauthorized changes to data on an IS. Users must not intercept or attempt to intercept or access data communications not intended for that user, for example, by "promiscuous" network monitoring, running network sniffers, or otherwise tapping phone or network lines.

c) **Disguised use**. Users must not conceal their identity when using IS, except when the option of anonymous access is explicitly authorized. Users are also prohibited from masquerading as or impersonating others or otherwise using a false identity.

d) **Distributing computer viruses**. Users must not knowingly distribute or launch computer viruses, worms, or other rogue programs.

e) **Modification or removal of data or equipment**. Without specific authorization, Users may not remove or modify any DMDC-owned or administered equipment or data from IS.

f) **Use of unauthorized devices**. Without specific authorization, Users must not physically or electrically attach any additional device (such as an external disk, USB virtual drive [storage device], printer, Personal Digital Assistant [PDA], CD-RW, or video system) to IS; in essence, no device that has the potential or ability to record, capture, affect, modify, alter, divert, or otherwise access DMDC information assets may be used without specific legitimate authorization.

g) **Use of Peer-to-Peer (P2P) software or networks**. Users must not use P2P file-sharing applications, such as BearShare, Kazaa, LimeWire, etc., except those that have been explicitly authorized by the DAA.

5) **Use in Violation of Law**. Illegal use of IS – that is, use in violation of civil or criminal law at the federal, state, or local levels – is prohibited. Examples of such uses are: promoting a pyramid scheme; distributing illegal obscenity; receiving, transmitting, or possessing child pornography; infringing copyrights; and making bomb threats.

With respect to copyright infringement, Users should be aware that copyright law governs (among other activities) the copying, display, and use of software and other works in digital form (text, sound, images, and other multimedia). The law permits use of copyrighted material without authorization from the copyright holder for some educational purposes (protecting certain classroom practices and "fair use," for example), but an educational purpose does not automatically mean that the use is permitted without authorization.

6) **Use in Violation of the DMDC Policy**. Use in violation of other DMDC policies also violates this IS Use Policy. Relevant DMDC policies include, but are not limited to, those regarding sexual, racial, and ethnic harassment.

7) **Use in Violation of External Data Network Policies**. Users must observe all applicable policies of external data networks when using such networks.

d. **Personal Account Responsibility**. Users are responsible for maintaining the security of their own IS accounts and passwords. Any password changes must follow published guidelines for passwords. Accounts and passwords are normally assigned to single Users and are not to be shared with any other person without authorization by the applicable Systems Administrator and the ISSO. Users are presumed to be responsible for any activity carried out under their IS accounts.

e. **Encryption of Data**. Sensitive data must be encrypted while in transit over data networks. Users are encouraged to encrypt files, documents, and messages for protection against inadvertent or unauthorized disclosure while in storage. DISSG must approve all encryption software and protocols.

Email Use

Using email for other than government approved official purposes (e.g., personal uses) will be kept to an absolute minimum, and will not interfere with the daily performance of one’s duties.

Email is subject to the Freedom of Information Act and the Privacy Act of 1974. Before sending email, you should consider that email is not private. Your email is an official record and is property of the Department of Defense. Your email can and may be monitored.

Only government email addresses should be used for work-related email. Personal email accounts are NOT to be used for transmission or storage of government email.

Power off your workstation

It is DMDC policy to turn off computers when you leave for the day. If the machine is left on (even when you log off), it is vulnerable to potential security issues. Hackers use unattended PCs to launch attacks on other systems. Also, it only makes sense to shut off the computer and especially the monitor when you leave for the day to save energy recent report noted significant savings if this was done. Note this is not just a DMDC policy - many other organizations such as business and even colleges have similar policies.

Lock Your Workstation

Locking your workstation when you leave your work area is DMDC Policy. Your name and account are tied to your workstation and when it is left unattended, someone else could use it with your name. If you are on the new W2k workstations, removing your CAC automatically locks your workstation.

Internet Usage Policy

Internet access must be either work related or incidental access done on your own time. Extensive access to the Internet on work time is not allowed. In addition, there are sites on the Internet which are not consistent with the use of a government computer system. The following list identifies prohibited uses:

- Visiting sites involving pornography.
- Gambling, conducting illegal activities, and soliciting for personal gain.
- Downloading copyrighted software without express permission.
- Downloading files without ensuring protection against viruses.
- Misrepresenting personal opinion as official information.
- Engaging in chain letters.
- P2P file-sharing.
- Capturing or listening to streaming audio such as Internet radio.
- Capturing or viewing streaming video such as Internet movies.
- Use of Internet instant message utilities such as ICQ, AIM (AOL Instant Messenger) or Microsoft NetMeeting.
- Use of real-time stock market tickers, sports scoreboards or other similar utilities that update information in real-time.

Internet usage at DMDC is monitored and leaves a clear audit trail. Those who do not follow the policy - either by excessive non-business usage or by access to prohibited sites - will be subject to administrative action. The Internet is an important tool in getting the government's business done and we have to be careful to ensure that it is used prudently.

CD and DVD Recording Policy

Creating CDs and DVDs is restricted to business uses. Users are prohibited from reproducing or duplicating any forms of artistic work or other forms of creative expression that are protected by copyright. This includes, but is not limited to graphics, images, photographs, literary works, software, video, and music.

The CD-Rs and CD-RWs should NOT be used to duplicate media across the LAN. This means that you cannot have the source media on a workstation different from where the CD-Writer resides or from a shared network drive. These situations would require the data to be pulled across the network.

POLICY 2.4 – Computer and Operation Management Policy

2.4 Policy Statement

General computing resources, including infrastructure, servers, desktops, and notebooks will be managed by STS. Equipment will be secured and configured in conformance with all Federal and DOD requirements.

Switch and Router Configuration Policy

This document indicates when a change request is required for configuration changes on a switch or router. All changes not listed below will require a Change Request to be submitted and approved. For non Change Request changes, each local site is required to maintain a change log for tracking purposes. This log must provide: date of change, purpose of change, and administrator who implement the change.

Switch procedures –

The following configuration changes to a switch do not require a Change Request.

- Port speed configuration
- Port duplex configuration
- Port VLAN assignment
- Port description/name
- Counter reset
- Span port assignment

Router procedures –

The following configuration changes to a router do not require a Change Request.

- Counter reset

Firewall Policy

1. The firewalls are installed in physically secured, limited access, environmentally controlled areas. Logical access to the firewalls is limited to the console interfaces or terminal access from specified administrators systems.
2. The selection of the firewall administrators must be approved by the Network Infrastructure Manager (who serves as the Network Security Officer) and the Systems Division Chief. Firewall administrators must be vetted at ADP-1.

3. All firewall hardware, firmware, configuration, and rule changes fall under Configuration and Change Management. These changes must be approved by the Technical Review Board and the Configuration Control Board. All approved changes are strictly based upon real business requirements weighed against security threats. All changes must be fully documented.
4. Firewall changes are normally scheduled with the Short Term Planning Board. Any emergency changes occurring outside the approved change window must be approved by the Systems Operations Chief or the STS Chief.
5. Firewall administrators will follow the guidelines in the DISA Network Security Technical Information Guidance. Any exceptions to these guidelines must be approved in writing by the STS Chief and the IAO and attached to this section.
6. All firewall rules must be reviewed every six months for continued applicability.
7. Firewall passwords will be changed every 90 days and whenever a person with access to the current firewall passwords is terminated.

POLICY 2.5 – Audit & Compliance Policy

2.5 Policy Statement

All DMDC IS must include sufficient means to reconstruct or review system and user system activities related to operations, procedures, or events occurring on the DMDC network and systems.

Audit data will be collected and stored in accordance with all Federal and DOD requirements. This includes periodic review of security-related logs.

Issue Statement

DMDC's audit policy requires a means to reconstruct and/or review user activities related to operations, procedures, or events occurring on the DMDC network and systems. To accomplish this, a record of activity or "audit trail" of system and application processes and user activity of systems and applications must be maintained. In conjunction with appropriate tools and procedures, audit trails can assist in detecting security violations, performance problems, and flaws in applications.

Organization's Position

Federal and DMDC directives require users to be identified, authenticated, and a record of users' activity be maintained and such that they can be held accountable for their actions. In addition, periodic on-line monitoring of user and system administration activities is required.

Applicability

These procedures apply to all personnel who use, manage, design, or implement programs on the DMDC network or DMDC IS.

Audit Trail policy

Audit features will log significant security events that could affect the DMDC security posture. The following functions must be recorded:

- Login attempts
- Change of logs, permissions
- System administrator activities
- Password changes, and
- File creations, changes, and deletions (critical systems and files only).
- The audit trail event record should specify:
- Type of event,
- When the event occurred,

- User ID associated with the event, and
- Program or command used to initiate the event.
- Audit trails must be reviewed monthly by the ISSO or other authorized Organization individuals who are not regular users and who do not administer access to the network.
- Anomalies must be immediately reported to appropriate supervisory and/or ISSO for follow-up action. All audit files will be stored in a secured room and kept for six months.

Compliance

Unauthorized personnel are not allowed to see or obtain sensitive data. Gross negligence or willful disclosure of DMDC sensitive information can result in misdemeanor or felony prosecution resulting in fines, imprisonment, civil liability, and/or dismissal.

Network Scanning and Probing

Any scanning, probing, O/S fingerprinting, denial of service attack or mapping of the DMDC LAN is considered to be an illegal activity and will trigger an incident report.

Any form of intelligence gathering, vulnerability or risk assessment, systems testing and evaluation (ST&E) or security certification by DMDC Systems staff, contractors or other DOD agencies must have prior approval from the DMDC Information Security Group (DISSG). A report will be submitted to the Information Systems Security Officer (ISSO) detailing the techniques to be used and the duration specified.

After written approval from the ISSO, notification of the intent to scan will be limited to management. Management will insure the disaster recovery system is tested and available in the event of damage or loss.

System Scanning Guidelines

Overview

IT Security at DMDC is an important aspect of our total organization. Without it, we are vulnerable to attacks from both within and outside of our enterprise. Isolated attempts to implement security can be fruitless, because IT security is dependent upon the total asset security; therefore, one weak link can bring down the entire system. Security functions must be centralized and distributed throughout the entire enterprise in a methodical and efficient manner.

To this end, DISSG was chartered to oversee and implement IT security throughout the DMDC enterprise. DISSG represents the organization on all security matters.

Packet/port scanning and Associated Analysis

Application owners in DMDC can be assured that their systems will be scanned on a regular basis to determine if they are vulnerable to common hacks. This assurance is provided by the regular Certifications and Accreditations (C&A) performed on all DMDC applications. Applications undergoing Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) will be scanned, and assessed, at least two times per C&A, to determine if they are sufficiently 'locked down'.

C&A scans and the associated vulnerability assessment will occur at least every 3 years, but usually more often, due to application upgrades. These scans are performed using independent auditors, and the results are documented in the Comprehensive DIACAP Package (CDP). A machine, system or even an entire network, at any site, can be the target of a scan.

If a system undergoes no major changes which require a new DIACAP then the next DIACAP scanning associated vulnerability assessment is due three years later. If this period of time is determined to be excessive, then functional IAOs should schedule a diagnostic system scan through DISSG.

Scanning systems in the DMDC enterprise is only allowed through DISSG. Scanning systems without DISSG permission is considered unauthorized and will be referred to the appropriate government authorities.

DISSG may scan and assess any DMDC system at any time, as required. These assessments include planned cyclical scans designed to monitor policy compliance, as well as targeted spot checks to determine security compliance. Internal scans may be unannounced.

POLICY 2.6 – Asset Classification and Control Policy

2.6 Policy Statement

Positive asset control procedures must be in place throughout the life-cycle of IT equipment. All information assets of a sensitive nature should be appropriately labeled and controlled.

Media Controls

DMDC shall ensure all media (e.g., diskettes, external drives, and master copies of software) containing sensitive information, including backup media and removable media, are stored in a secure location when not in use. DMDC shall ensure backup media are stored offsite in accordance with their contingency plans. All media shall be marked with the appropriate sensitivity level of the information stored on the media.

Labeling

Classified email and paper memos should include labels in the subject field. Labels for classified information should appear on floppy diskettes, magnetic tape reels, CD-ROMs, audiocassettes, USB devices, and other storage media. If a storage volume (such as a floppy diskette) contains information with multiple classification levels, the highest classification should appear on the outside or overall label. Likewise, when creating a collection of information from sources with various classification levels, the collection must be classified at the highest classification level of the source information.

Printing, Copying and Fax Transmission

Destruction of Waste Copies

If a printer, copier, or fax machine jams or malfunctions when printing sensitive or classified information, the involved users shall not leave the machine until all copies of the sensitive/classified information are removed or are no longer legible. All paper copies containing any sensitive or classified information shall be disposed of by shredding or other methods approved by DISSG. Documents classified as FOUO or DOD Sensitive should be placed into Shred-it bins for destruction.

Faxing Precautions

Sensitive materials shall not be faxed unless: (1) an authorized staff member is on-hand at the time of transmission to properly handle the materials at the receiving site, (2) the fax is sent to a locked room to which only authorized workers have access, or (3) a password-protected fax mailbox is used to restrict release to an authorized recipient. Sensitive information shall not be faxed via untrusted intermediaries (hotel staff, rented mailbox store staff, etc.). As the tables accompanying this document indicate, classified information may only be faxed if the connection is protected with encryption systems approved by DISSG. Confirm reception of sensitive or classified information via fax promptly.

Printer Precautions

When printing sensitive information, the user shall: (1) be present at the printer at the time of printing to prevent the information from being revealed to unauthorized parties, or (2) direct the output to a printer inside an area where only authorized workers are permitted to go.

Clearing of Media

Sanitization of Hard Drives

DMDC shall ensure that any sensitive information stored on media to be surplused or returned to the manufacturer shall be purged from the media before disposal. Disposal shall be performed using approved sanitization methods. DMDC shall maintain records certifying that such sanitization was performed.

Persistent memory USB devices will be treated as removable media and, in accordance with DODD 5200.1-R; the devices will be secured, transported, and sanitized in a manner appropriate for the classification level of the data they contain. This includes any device with internal non-removable persistent memory, not just thumb drives or disk drives.

Magnetic media containing classified information can be sanitized by use of an approved degaussing procedure. The DAA with the Data Owner’s approval (if applicable) can allow overwriting of some types of classified information as a sanitizing procedure.

Disposal Policy

DMDC shall establish procedures to ensure sensitive information stored on any media is transferred to an authorized individual upon the termination or reassignment of an employee or contractor. DMDC shall ensure sensitive information is purged from the hard drives of any workstation or server that is returned to the surplus pool of equipment or transferred to another individual (e.g., returned to the manufacturer). DMDC shall ensure all media containing sensitive information (e.g., paper, diskettes, and removable disk drives) are purged in such a manner that all sensitive information on that media cannot be recovered by ordinary means. Disposal shall be performed using approved sanitization methods. DMDC shall maintain records certifying that such sanitization was performed. Examples of methods of disposal are crosscut shredders, degaussing, and approved disk-wiping software.

Degaussing

Degaussing, also referred to as demagnetizing, is a procedure that reduces the magnetic flux density to zero by applying a reverse magnetizing field. Degaussing renders any previously stored data on magnetic media unreadable. Degaussing is the most reliable method of purging magnetic media short of destruction. Only NSA-approved degaussers will be used to destroy sensitive data stored on magnetic medium.

The list of magnetic degaussers that satisfy the requirements in NSA/CSS Specification L1 4-4-A is included in NSA's Information Systems Security Products and Services Catalogue as the degausser products list (DPL). The catalogue is updated quarterly and is available through the U.S. Government Printing Office (GPO).

The DMDC ISSO, with concurrence from the Data Owner, will make the final determination regarding the necessary destruction means.

Destruction of Sensitive Data

All magnetic removable media considered for disposal will be destroyed. Prior to destruction, media will be sanitized– all prudent and necessary measures shall be taken to ensure data cannot be retrieved through known conventional or unconventional means.

Magnetic removable media containing sensitive data such as diskettes, zip disks, optical tape, optical Bernoulli cartridges, and optical disks: Read Only (including CD-ROMs); Write Once, Read Many (WORM); Read Many, Write Many; Digital Video Disk (DVD); will be destroyed. CDs will be destroyed by scratching both surfaces with some abrasive substance to render the CD unreadable prior to breaking the CD into numerous pieces with some type of impact devices. All other types of magnetic removable media will be sanitized using COTS, GOTS, or DMDC-approved software, prior to being physically destroyed.

Media having ever contained classified cannot be sanitized by overwriting; such media shall be degaussed before destruction.

Storage and Disposal of Cryptographic Modules

Introduction

This policy provides guidance for the storage and disposal of cryptographic modules, such as Chrysalis Hardware Security Modules (HSM), nCipher HSM, and Smartcards that are used to access control and administer nCipher and Ingrian units. The policy also applies to hard disks containing applications and logic to clone Chrysalis HSMs.

Background

There is not an explicit DOD policy pertaining to the storage and disposal of unclassified cryptographic modules. However, similar controls as specified in the DOD X.509 Certificate Policy (12 December 2002) should be used.

The functional components that interact with cryptographic modules are the Key Management Station (KMS), Issuance Portals (IP), and the SSL accelerators (Ingrian/nCipher). The KMS is a stand-alone machine that can create, edit, and copy HSMs to be used by the IPs. The operating system and application software is on a removable drive, which also needs to be managed securely.

The IPs reside between the local Registration Authority (RA) and the Certificate Authority (CA) and function as either a secure proxy or secure delivery change. The SSL accelerators use HSM and smartcard tokens to control operation and allow administrative access.

An RA or LRA requesting a CLASS 3 certificate expects the providing CA to be governed by the DOD X.509 Certificate Policy, thereby providing an appropriate level of assurance. If the request is going through an intermediary (the IP), it is expected that the intermediary provide assurance no less than the CA. Hence, much of the X.509 Certificate Policy for physical, administrative, and technical controls are relevant to the CAC Issuance Portal system.

Production Sets

Storage

Store the cryptographic modules in a secure controlled access site with the following characteristics:

1. Access limited to personnel filling Trusted roles.
2. Inventory control processes to manage the origination, arrival, condition, departure, and destination of each device.
3. All physical access attempts recorded in an event journal.
4. Incident processes to handle abnormal events and security breaches.
5. Audit processes to verify effectiveness of controls.

Installation

Perform in the presence of no less than two individuals in Trusted Roles.

Removal

Perform in the presence of no less than two individuals in Trusted Roles.

Disposal

If the device is still functional, the HSM should be zeroized prior to disposal. All disposed HSMs should be physically destroyed.

If functional, removable hard disk drives should be sanitized using file overwrite software that prevents recovery. All removable hard disk drives (functional or not) should be disabled (cut wires, connectors, etc.) and then destroyed at an appropriate facility.

Test Sets

Although these do not contain operational key sets, the test sets still contain the same software and algorithms as production sets and therefore are handled much the same as production units.

Storage

Store the cryptographic modules in a secure controlled access site with the following characteristics:

- Access limited to personnel filling Trusted roles.
- Inventory control processes to manage the origination, arrival, condition, departure, and destination of each device.
- All physical access attempts recorded in an event journal.
- Incident processes to handle abnormal events and security breaches.
- Audit processes to verify effectiveness of controls.

Installation

Not applicable, provided the unit operates in a controlled environment.

Removal

Not applicable, provided the unit operates in a controlled environment.

Disposal

If the device is still functional, the HSM should be zeroized prior to disposal. All disposed HSMs should be physically destroyed.

If functional, removable hard disk drives should be sanitized using file overwrite software that prevents recovery. It is not necessary to physically destroy a functional test hard disk that has been sanitized.

If not functional, the hard disk drive should be disabled (cut wires, connectors, etc.) and then destroyed at an appropriate facility.

Storage Containers

A commercial safe can be used to store HSMs provided there is an access and audit procedure that conforms to the storage recommendations above.

Notebook Policy and Checkout Procedure

DMDC Management has specified a limited number of notebook computers for staff use. Each Division Chief has been allocated a set number of notebooks. Assignment and use of these notebooks are at the discretion of the Division Chief.

Notebook Distribution

Leadership Development Program

The Leadership Development Program members are assigned a notebook computer.

Specialized Use

Some notebooks have been procured and dedicated for specialized use - network monitoring, development, special projects. These notebook computers have high compute and processing capabilities similar to high end desktops but are used where mobility is required.

General DMDC Support

All remaining notebooks are to be in an inventory for check out. Authorized purposes for checkout include: TDY, attending training where a notebook computer is required, special short term project, etc. Typically checkout is one to two weeks duration. While there is expectancy for the notebook to be returned within that period there is some flexibility, recognizing that staff members are often busy upon return from TDY. Notebooks that have not been returned within the time period allocated are subject to being recalled at any time.

Checkout Procedure

Request checkout of notebook computers from the STS Helpdesk. At the time of the request, note any special software or hardware requirements. Requests should be made at least one in advance to provide time to locate, configure, and test the notebook. Requests should specify the length of time you will require the notebook. Quantity of notebooks and the length of the check out time may be restricted. These constraints will be defined in the Equipment Checkout Receipt form.

If a notebook computer is unavailable, the Helpdesk will recall notebooks with an overdue status.

Availability

Notebook computers are available on a first-come, first-serve basis. Depending on the availability of notebooks, you may not receive the exact model you requested. Demand may exceed what can be provided.

If none are available (all checked out recently), the Helpdesk will notify you.

You can work this out with your Division Chief, who has been provided an allocation of notebooks at his or her disposal. There are several solutions for saving data from the notebooks. All the notebooks have read and write CD capability for data backup and removal prior to turning in or exchanging to facilitate equipment sharing. In addition to CD, if necessary, each Division has its own set of ZIP drives with their Tech Rep to keep data and drivers can be added to support ZIP technology. Each Division also has memory chip thumb drives for temporary storage to transfer data. The hard drive in the notebook is also removable. Systems can also provide a Division Chief, a second notebook computer hard drive to swap the hard drive in special situations.

Priorities

Requests are generally filled on a first-come, first-serve basis. However, allocation may also be determined by division funding levels. If your division budgets dollars for IT related items, STS can track your purchases and similarly get equipment and resources to your staff quicker than non-budgeted equipment.

Broken Notebooks

If a computer breaks while checked out, immediately return it to the Systems Helpdesk. If it is under warranty, it will be sent out for repair. Notebooks that are out of warranty are generally not cost effective to repair. Replacement of the loaned notebook is subject to the current availability of notebooks. No repairs, modifications, alterations, or changes are to be made to the issued equipment, except as authorized by, and accomplished at the specific direction of the STS Chief.

Check In Procedure

Employees are expected to return the notebook and any accessories to the STS Helpdesk by the agreed return date. If for any reason you are unable to return the notebook as expected, please contact the Helpdesk. All equipment must be returned within 24 hours of demand by any authorized Division Manager. Any notebooks must be returned immediately upon termination of employment, for any reason.

Notebook Use

The equipment remains the property of DMDC and is not to be sold, traded or loaned to any individual outside or inside the agency. The equipment is loaned for the sole benefit of DMDC. It is not to be used for commercial purposes, personal financial gain or in the pursuit of interests contrary to the welfare of the agency. Use of the equipment shall not violate DMDC computer use policy. By signing the Equipment Checkout Receipt, the employee accepts full responsibility for the equipment, and agrees to protect the equipment from damage and harm. Also, the employee assumes financial responsibility for the repair or restoration of any damage caused through neglect or abuse of said equipment, or replacement in kind for loss, theft, fire or natural or unnatural disaster. The employee will not be charged for normal wear and tear of the equipment. The decision of the STS Division Chief will be final in all disputes.

Virus Protection

All media disks must be scanned for viruses prior to their use. There shall be no exceptions to this practice. Contact the STS Helpdesk to obtain instructions on how to use the antivirus software. Antivirus software must be enabled at all times.

Firewall Protection

All DMDC notebook computers must have the personal firewall software enabled at all times. There shall be no exceptions to this practice. Contact the STS Helpdesk to obtain instructions on how to use the firewall software.

POLICY 2.7 – Business Continuity Planning

2.7 Policy Statement

Business continuity must be considered in the design and operation of all critical systems.

POLICY 2.8 – Account Management

2.8 Policy Statement

All persons granted access to DMDC resources are responsible for the safeguarding of their network credentials. Account use is audited and individuals are responsible for all actions occurring using their credentials. Access to specific systems or applications is only granted to persons needing it to support specific work.

Network accounts will only be enabled for users that have:

1) been vetted at the appropriate level for their access as per DMDC SOP;
2) completed Security Awareness training;
3) completed Privacy Act training;
4) executed the DMDC Information Systems User Agreement.

Account Management Policy

STS manages users' accounts by: creating accounts; blocking or deleting accounts; managing user rights; and ensuring adherence to password policy.

Users are only provided access to servers, desktops, and hosts to support specific job-related functions. All new employees receive a Windows domain account and email access based on the Employee Action Request form. DMDC Division Chiefs authorize accounts on Unix servers via the Account Request form. Division Chiefs authorize Oracle accounts via the New Database Project form.

Accounts created for consultants should be disabled or deleted on the day of their departure. The DMDC associate overseeing the consultant should notify STS immediately when personnel depart per the Personnel Termination Policy.

Accounts created for external users should be temporary accounts and set to expire after 180 days or at the end of the requirement whichever occurs first. Accounts that are needed for longer periods must be reauthorized every 180 days. This will allow DMDC to proactively reconfirm the requirement and update information about the use of the account. Managers of these accounts must keep records that will stand up to future security audits.

Where possible, user account names will be the first six letters of the last name, first initial of first name, and first initial of middle name. Where there is no middle name, N is used.

Accounts are not to be shared and associates will not allow others to use their individual accounts. Accounts will be suspended if unused for more than 30 days. Suspended Reactivation will be done via a Helpdesk request.

Workstation Security:

- Users will **lock** their machines when they leave their desk.
- When leaving for the day, users will **shut down** their computers.

DMDC Division Chiefs or their representative notify STS via the Help Desk or the Employee Action Request form when employees leave DMDC or leave projects that authorize them access to DMDC servers, desktops, host systems and Oracle. When accounts have been disabled due the departure of an associate, the Division Chief may request that STS transfer data out of these accounts as necessary to ensure that the related work can continue.

Windows domain, Exchange, Unix, and Oracle accounts will be disabled immediately upon an associate's departure and will be deleted within 30 days after receiving an Employee Action Request from the respective DMDC Division Chief. Unused accounts will be disabled after 30 days of inactivity and deleted after 60 days.

Account Termination Policy

Purpose

This document defines the account termination policy for DMDC. This policy has been created to ensure security within the DMDC environment by providing that all user accounts are promptly terminated upon the departure of an employee.

Scope

This policy applies to DMDC and pertains to all assets under the accreditation boundary as defined by the DAA.

Responsibilities

STS shall be designated as the maintainers of user and access control information. These duties shall include the creation, deletion, and maintenance of user accounts and change of access controls when necessary. Users whose association with DMDC is terminated shall have their access privileges to DMDC resources immediately revoked. Administrators shall arrange for the users programs and other data to be archived, as well as create procedures for revoking user access. DMDC Division Chiefs or their representative shall notify the Systems and Technical Support division in a timely manner when employees leave DMDC, or leave projects that authorize them access to DMDC assets and or applications. The notification shall include the termination type, which will distinguish between an employee initiated (voluntary) separation and an employer initiated (involuntary separation) termination. An automated notification method shall be used wherever it is available.

Voluntary Separation

Voluntary Separation occurs when the termination is employee initiated. Accounts created for all employees will promptly expire upon notification of termination. Upon request, Systems will work with the respective divisions to transfer data out of these accounts as necessary to ensure that the related work can continue. All accounts will be deleted within a reasonable time of receiving notification of an employee termination from a DMDC Division Chief or their representative. If necessary, backups of all systems that the employee had administrative control over shall be made and held for a period of six months. DMDC Division chiefs or their representatives shall determine if there are any access storage media issues used by the departing employee, which may require additional attention.

Involuntary Separation

In the event of an employee termination due to adverse circumstances, all system access shall be deleted the day of the employees' departure. If an employee is to be fired, all system access shall be removed at the same time, if not before, the employee is notified of their release.

Account Reviews

Systems and Technical Support shall perform expected audits of user accounts and associated access controls to ensure validity and accuracy. Regular reviews will be performed to identify dormant accounts. Dormant accounts, or those accounts which have not been accessed for 60 days without sufficient reason, will be suspended. Reactivation will be done via a Helpdesk request.

External User Accounts

Accounts created for external users will have an expiration date. This date shall be set based on the end of the requirement, or if the requirement is ongoing set to 180 days. This will allow DMDC to proactively re-confirm the requirement and update information regarding the use of the account. External user accounts, when applicable, will be controlled and monitored. Managers of these accounts must keep records that will stand up to future security audits.

Verification

The Systems and Technical Support Division shall be responsible for verifying that all system access has been terminated for every separating employee. This verification process shall ensure that each account for every terminated employee has been expired or otherwise deleted in a timely manner.

Password Management Policy

Overview

In order to grant access privileges and attain individual accountability, it is necessary for any IT system to be able to uniquely identify and authenticate each person who uses it. In many cases, a password scheme will be used to achieve this. The security provided by a password system depends on the passwords being kept secret at all times. A password is vulnerable to compromise whenever it is used, distributed, stored, or even known.

Passwords are the front line of protection for user accounts. A poorly protected or poorly chosen password may result in the compromise of DMDC's entire network. As such, this policy prescribes steps to be taken to minimize the vulnerability of passwords.

Purpose

The purpose of this policy is to establish a DMDC standard, for the creation, distribution, storage, protection, transmission, and use of passwords.

Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any DMDC facility, has access to the DMDC network, or stores any non-public DMDC information.

Policy

Password system must be able to uniquely identify each individual user of the system. Each user ID should be assigned to only one person. No two people may ever have the same user ID at the same time. Password systems must assure unequivocal authentication of the user’s claimed identity.

Password Protection

Passwords will be protected in an appropriate manner at all times. This includes, but is not limited to creation, distribution, transmission, authentication, and storage. Passwords will be encrypted. Decryption of passwords will not be possible. Password authentication will be performed by encrypting the user-supplied password and comparing it to the stored encrypted password.

Users shall not share a fixed password with anyone, including their manager or co-workers. Instead, Users shall employ authorized mechanisms to share information such as local server shared directories, electronic mail, intranet pages, or floppy disks. Users shall not store their passwords in any computer files such as scripts or computer programs. Likewise, passwords shall not be written down unless a transformation process has concealed them, or they are physically secured (such as placed in a locked file cabinet). All default passwords set by the hardware or software vendor shall be changed before the involved system is placed into production.

Password System Set-Up

All computers permanently or intermittently connected to DMDC networks shall have password access controls or other approved authentication methods such as Smart Cards. Multi-user systems shall employ user-IDs and passwords unique to each user, as well as user privilege restriction mechanisms. Network-connected single-user systems shall employ hardware or software controls approved by the ITSEC Team that prevent unauthorized access including a screen blanker triggered by a certain period of no keyboard activity.

Computer and communication system access control shall be achieved via passwords that are unique to each individual user. Access control to files, applications, databases, computers, networks, and other system resources via shared passwords (also called "group passwords") is prohibited.

Password Control

User IDs and passwords provide unique identifiers that enable a system to identify authorized users. Users must maintain exclusive control and use of their password and protect it from inadvertent disclosure to others. Passwords will be kept private, i.e. not shared or coded into programs or scripts. Passwords will not be written down or stored on desktops, in desk drawers, on post-it pads (*stickies*), etc., where compromise is likely. Any password written down must be secured in a sealed envelope and stored in a locked safe or other approved secured container. All passwords shall be immediately changed if they are suspected of being disclosed.

Password Generation

Initial passwords should be randomly generated in accordance with CSC-STD-002-85.

The initial password must not be exposed to the administrator after it has been generated. Generic password assignment is prohibited. Initial passwords should be securely transmitted to the user, and user should immediately change password upon receipt.

Password Transmission

Passwords will be encrypted prior to being transmitted. Protect passwords during transmission at the same level required for the system or data that the password is protecting.

Password Storage

Stored passwords must be encrypted in compliance with CSC-STD-002-85.

Screen Saver Settings

Password protected screensavers should be enabled and set with an appropriate activation delay.

Password Aging & Management

All default "system" passwords will be removed/changed/reset. Delete all unnecessary accounts and change all passwords included in a newly acquired system before allowing any user access to the system.

Password Change Authorization

Password change procedure should be invoked at the user's request and should not require administrator intervention.

Password Expiration & Reuse

Passwords should be set to expire at least every 180 days.

Log-In Attempts

Accounts should be locked after 3 unsuccessful login attempts. Administrator should be notified in real-time of failed login attempts. The administrator should receive immediate notification in the event of several consecutive login failures. Upon successful login, users should be notified of the location, date, and time of the last successful login, as well as any failed login attempts.

Failed Log-In System Response Statement

The system response statement should not reveal the details of the failed log-in. Instead, a generic statement should be reported.

Account Inactivity

The administrator must lock or remove accounts immediately after employee termination or suspension. The system should automatically lock accounts after a specified period without a successful login.

Auditing

System audit functionality should be enabled, where possible, to track successful logins, login failures, and password changes.

User Security Awareness Training

Administrator will assure that all users have annual security awareness training, which will address user responsibilities. Prior to the issuance of passwords, users must take appropriate training regarding the protection of their user ID and password, along with other pertinent security issues.

User Responsibilities

- Passwords should not be written down or sent in email.
- Passwords should be kept secret.
- Passwords should not be shared.
- Passwords should not be given out. (Not even to the help desk.)
- Passwords should be memorized. They should not be stored in any form.
- Inform DISSG if anyone (including the help desk) asks for your password.
- Never leave a system unattended while logged in. Always log out when leaving the system for any period of time.
- Password protected screensavers should be enabled and set with an appropriate activation delay.

Password Composition

- Passwords generated by the user must meet the criteria outlined in the DMDC SOP.
- Passwords must mix both upper and lower case characters.
- Passwords must contain at least one numeric and one special character.
- Passwords will be a minimum of 8 characters.
- Passwords and user logon IDs will be unique to each authorized user.
- Passwords will be kept private. Users may not give their passwords to other users.
- DON'T use your login name in any form (as-is, reversed, capitalized, doubled, etc.).
- DON'T use your first, middle, or last name in any form.
- DON'T use your spouse or child's name.
- DON'T use other information easily obtained about you. This includes license plate numbers, telephone numbers, social security numbers, the make of your automobile, the name of the street you live on, etc.
- DO use a password that is easy to remember, so you don't have to write it down.
- DO use a password that you can type quickly, without having to look at the keyboard.

Methods of selecting a password that adheres to these guidelines include: Choose a line or two from a song or poem, and use the first letter of each word. Alternate between one consonant and one or two vowels. This provides nonsense words that are usually pronounceable, and thus easily remembered. Remember to comply with the DMDC policy. Your password must contain numeric and special characters and must have a mixture of case for the alpha characters.

Enforcement

Any employee, (including contractors and vendors with access to DMDC systems), found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

POLICY 2.9 – Privacy Act and Other Sensitive Data

2.9 Policy Statement

Privacy Act and other sensitive data entrusted to DMDC must remain protected at all times. This includes receiving and sending of that data, as well as when that data is at rest on a storage device and any other time the data is removed from the workplace to accomplish authorized work.

Privacy Act data and other sensitive data must not be stored on personal IT devices. All persons with access to Privacy Act data must be vetted as ADP-II or higher.

DMDC will provide access to non-public data, i.e. sensitive and proprietary data, to persons or organizations who: 1) have a legitimate Need-To-Know (NTK), as determined by DMDC; 2) have the proper vetting level or clearance for the specific information; and 3) have procedures and information security measures in place to assure the confidentiality and integrity of the information.

Non-public data must only be exchanged in a secure manner. When transmitted electronically, including via email, non-public data must be encrypted.

Violations of this policy may result in disciplinary action.

2.9.1 Scope

This policy applies to all persons and organizations that access or use DMDC data, including those affiliated with third parties who access DMDC computer networks.

2.9.2 Definitions

Sensitive Data. Sensitive data is any item, collection, or grouping of information whose unauthorized disclosure could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national interest.

In general, if an employee believes the data set may be sensitive, it should be treated as such. Division chiefs have final determination as to what data should be categorized as sensitive.

Privacy Act Data. Privacy Act data is a special class of Sensitive data. It is often referred to as Personally Identifying Information (PII) and is defined as:

Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. (OMB 07-16)

Although Privacy Act data is a special class of Sensitive data, it requires additional controls for transfer or access.

In no case shall DMDC sensitive data of any type be stored on personal IT devices.

2.9.3 Implementation

This section presents the detailed policies for Sensitive and Privacy Act data.

2.9.3.1.1 Privacy Act Data

Privacy Act data must be protected during transit. The following rules apply to the transport and use of Privacy Act data.

Requirements for Digital Data

1. All Privacy Act data sent to or from DMDC in digital format must be transported using government owned equipment and materials provided by DMDC and MUST BE ENCRYPTED using approved techniques. This includes but is not limited to, data transfers across all lines including dedicated T1's, CD's, floppy disks, thumb drives, e-mails, attachments to e-mail, laptops, and tapes.
2. All processing of Privacy Act data at DMDC will be done on government owned equipment.
3. Privacy Act data will not be placed on personal IT devices or media, including computer, PDA, thumb drive, etc.
4. Privacy Act data placed on a mobile government IT device will be encrypted.
5. Downloading, emailing or copying of Privacy Act information for any reason other than Official Business is prohibited.
6. All work on Privacy Act protected information and sensitive data will be done in a DMDC facility or via an approved secure remote desktop.
7. Privacy Act Information released on paper (i.e., via non-electronic means) must have a Privacy Act handling warning printed on the material and the material will be wrapped to prevent accidental exposure of data. While being handled in hard copy format, it must have a DD2923 cover sheet (see sample) indicating that it is subject to Privacy Act protection. The same process will be used for Sensitive but unclassified material.
8. All releases of Privacy Act data must be documented and approved for release in DMDC's Privacy Release Accounting System (PRAS).
9. If data is received which is not encrypted the following steps should be followed.
    a. The data should be protected according to this policy.
    b. The recipient should notify his/her Division Chief and DISSG.
    c. The sender should be notified that they sent the data in violation of DMDC policy and provided DMDC Memorandum dated 16 June 2006, Subject: Secure File Transfers which states that a second violation will result in DMDC not participating further in the data exchange.

Requirements for Printed Data

Information shall be protected from unauthorized disclosure throughout its period of transit. A DD2923 cover sheet (available on the iWeb), sealed envelopes, briefcases, etc., shall be used as necessary to ensure the protection of the information.

For mailed material, first class mail and ordinary parcel post may be used for transmission. The material shall be placed in a single sealed envelope or sealed single wrapping for transmission. Transparent envelopes or wrapping material, such as "shotgun" envelopes or heat sealed plastic containers, which might reveal the contents, shall not be used. Do NOT mark the envelope or wrapping with sensitive designators such as “For Official Use Only.” Bulky shipments, which qualify under postal regulations, may be sent by fourth class mail.

Data will be stored in an appropriately marked folder when not in use. Additionally, it will be kept in a locked facility when not under control of the user.

Printed data will not leave the work place without Division Chief approval.

2.9.3.1.2 Sensitive Data

Non-Privacy Sensitive data is categorized into three types – record-level, non-record-level, and operational-level.

Record-level. With record level data, each record in a file or database represents one individual.

Non-record-level. Non-record-level data is aggregated data and provides information such as counts of records, counts of attributes, statistics, etc.

Operational-level data. Operational-level data pertains to the security and functional operations of DMDC, such as network design, configuration information, vulnerabilities, security assessments, financial, procurement sensitive, etc. This type of data would typically be designated FOR OFFICIAL USE ONLY (FOUO).

Both record-level and operational-level sensitive data will be treated as Privacy Act data and all requirements listed above under Privacy Act data must be met.

Requirements for Digital Data

Non-record-level sensitive data, at a minimum, must be zipped and password protected prior to transfer or hand-carrying. An approved encryption technique is recommended but not required.

Non-record-level sensitive data will not be placed on personal IT devices of any kind (computer, PDA, thumb drive, etc.).

Non-record-level sensitive data placed on a mobile government IT device will, at a minimum, be password protected.

Requirements for Printed Data

All printed Sensitive data will be treated as if it were Privacy Act data and follow the requirements listed above for Privacy Act printed data.

2.9.4 Breach of Policy and Enforcement

Violations of this policy may result in disciplinary action.

POLICY 2.10 – IT Acquisition Policy

2.10 Policy Statement

All IT acquisition, either hardware or software, must comply with Federal and DOD requirements and be coordinated through DMDC management, the Developers Steering Group (DSG), the Integrated Development Group (IDG), the Technical Review Board (TRB), and DISSG.

Software Acquisition Policy & Procedures

Introduction

Below is the policy and process, which the Systems and Technical Support Division uses in considering a request for a new software product. By sharing publicly with all the members of our Enterprise network the steps in considering a request, everyone can be more familiar with our process.

Step 1. Check for Duplicate Software Solutions

Is there already a software solution for this application?

Step 2. Justification for New Software

If this requires a new category of software, could the proposed software be the standard for all sites? Could this software be part of the DMDC/DHRA software strategy, a solution for a specific area or category of application? If others needed software to accomplish this application, would it be the DMDC/DHRA solution in step 1?

The user may have identified a new category of solution but users also need to consider carefully whether the product has sufficient breadth, scope, and viability to be part of the DMDC/DHRA suite of software solutions. Users need to question - is the software being requested a point solution, narrow in scope, usable in only one specific area, for one person or one interest? Is this the best software for this category? Would it stand up to scrutiny from other users who would be employing this software to accomplish their work? What about the company - is there support?

In general, unless there is high justification, software requests for singular use will be rejected. This may seem harsh - what's the harm with buying just one little thing that only costs $100? There are many more costs, however, than just the procurement price.

- There is cost in the testing and integration of software for problems or conflicts with our hardware configurations or with the other existing approved products in our suite of software.

- Software has its own life cycle - it's not a one time cost - there are upgrades, plus the patches and bug fixes that need to be tested and then delivered to the almost 1000 workstations on our network. Also, new versions may be needed to match changes in the operating system, for example.

- With additional different new software there is the need for training and then also considerations on maintenance - who is going to use this and if this person is not here, who is going to be maintaining this person's stuff when they are gone?

- Software requests at the beginning for only one special person rarely stay that way. Information is shared; it is updated - which means other people will eventually also need copies, training, maintenance, installation - adding to the organizational cost of ownership for technology.

This is not meant to be negative but to provide the other side and our considerations - what people often do not see or understand when they feel they are making just a simple request to purchase a little software.

Step 3. Conflicts with Existing Solutions

Does this software conflict with existing solutions?

a) Technically?

b) Strategically?

In analyzing it in technical terms, we have to consider what the effect of the application is. If in order to use it, the software requires generating a lot of network traffic that hinders other applications, we would have serious reservations. Does it conflict with our standards? How does it need to be installed? Does it work with Novell, NT, Oracle? When it is installed does something else no longer work (for example, replacing existing DLLs)?

In strategic terms, we have invested in products that are considered a strategic part of IT and organizational strategic directions. We would not be interested, for example, now in buying new and competing solutions for database. Another example was the debate on using Microsoft Access. Systems advised that Access was just to be used for a standalone PC database. We instead supported client server methodologies. Users favored the easier to use Access but it was not client server. It was not scalable and it proved to be problematic for developers using it for network applications. Another example - recently our research determined that a product requested for web development worked only on IIS whereas our Web solutions are in UNIX. Selecting software that conflicts with the current strategy and directions will have a very high cost to the organization.

Step 4. Input From Users

Get input from other users. The myriad of users we have on our network share a wide range of knowledge and experience. If a user believes their product being requested passes the gauntlet to be worthy of being on the DMDC/DHRA approved software list, we will announce the product, its description, category, etc. for others who may have experiences or be knowledgeable of this product or other products they may believe to be better in this category. A lot may be learned that may save us much effort and time from an e-mail discussion group on the product and category.

Step 5. Product Evaluation

Based upon Step 4, an evaluation product will be requested. People interested in the product can work with Systems to test the product in a test environment.

Step 6. Product Installation

Product installation and distribution.

Conclusion

This may seem a long, arduous process. It is necessary but it does not have to be long. Depending upon the urgency, the process could be fairly quick. Also some steps could be accomplished in parallel.

POLICY 2.11 – Wireless Policy

2.11 Policy Statement

All wireless use must conform to DOD current standards. Wireless operation must be coordinated with STS and DISSG. Periodic compliance audits will be conducted by DISSG.

Wireless Strategy and Oversight

DMDC manages the acquisition and use of wireless technology in the same manner as other information technology (IT). There are four key bodies – the DMDC Developers Steering Group (DSG), the Integrated Development Group (IDG) the Technical Review Board (TRB) and the DMDC Information Systems Security Group (DISSG).

The DSG defines the enterprise standards for software platforms, development methodologies and procedures, configuration management, and testing/QA procedures. DSG is also responsible for knowledge sharing throughout DMDC as regards these standards and procedures.

The IDG is focused on software and represents a common approach to developing quality software for DMDC.

The TRB reviews and approves all changes to IT operations, including the introduction of wireless technologies, before being placed into production. The TRB has oversight responsibility for infrastructure and general purpose support systems (desktop, laptops, servers, database, etc.).

Wireless Acquisition

All introduction of wireless technology into existing systems and all new acquisitions must comply with the evaluation and validation requirements of DODD 8100.2 and DODI 8500.2.

If situations occur that require exceptions, a risk assessments must be performed and reviewed before any exception is granted.

Wireless Testing

Functionality of all products will be evaluated and specific operational configurations defined in a test environment. The testing process will follow the general strategy of:

- Evaluate suitability for application needs

- Evaluate product functionality
- Test functionality and security controls
- Develop prototype configurations
- Test and refine (iterative)
- Implement pilot test (limited roll-out)

Wireless DOD Knowledge Management Participation

The Knowledge Management (KM) process is used as a first step in identifying candidate wireless technologies. As wireless technologies are evaluated, DMDC will provide feedback to the wireless KM process concerning strengths, weaknesses, vulnerabilities, mitigation techniques and related security issues.

POLICY 2.12 – Data Security Policy

2.12 Policy Statement

All data must be protected at a level commensurate with the threat environment. The level of protection will comply with DOD policy and standards.

2.12.1 Scope

This policy applies to all DMDC and customer data assets that exist in any DMDC processing environment on any media during any part if its life cycle.

2.12.2 Rationale

DMDC is a “Data Center” -- data is our primary asset and should be protected in a manner commensurate to its value. Additionally, much of our data is subject to the Privacy Act and there is a legislative requirement to safeguard it. Unauthorized modification or disclosure of our data could compromise military personnel, cause financial loss, violate federal laws, cause privacy violations, violate business contracts, reduce credibility and reputation, and jeopardize our ability to perform our mission.

2.12.3 Policy Implementation

DMDC categorizes unclassified data as Public, Proprietary, or Sensitive. Public data requires no special precautions; however Proprietary and Sensitive data should be safeguarded using a combination of appropriate vetting processes, access controls, and cryptography.

Proprietary and Sensitive data shall only be accessible to explicitly identified, authenticated, and authorized entities with a need-to-know.

Specific safeguard requirements depend on whether data is being distributed or being stored in an Information System (IS).

2.12.3.1 Data for Distribution (includes removable media)

All data except Public data will be encrypted while being electronically transmitted. Likewise, data stored on removable media such as floppy disk, thumb drive, removable disk, CD/DVD-ROM, or magnetic tape will be encrypted.

2.12.3.1.1 Public Data

No special precautions are needed.

2.12.3.1.2 Proprietary Data

Proprietary data that is being electronically transmitted should be encrypted. It is desirable to use NIST-certified cryptography.

Prior to delivering Proprietary data to an external party, a Non-Disclosure Agreement (NDA) or Memorandum of Agreement (MOA) should be executed wherein the receiving party acknowledges the proprietary nature of the data and agrees to maintain appropriate safeguards.

2.12.3.1.3 Sensitive Data

Sensitive data that is being electronically transmitted must be encrypted using NIST FIPS140-validated cryptography.

Prior to delivering Sensitive data to an external party, a Memorandum of Agreement (MOA) should be executed wherein the receiving party acknowledges the Sensitive nature of the data and agrees to maintain appropriate safeguards.

2.12.3.2 Stored Data

2.12.3.2.1 Public Data

No special precautions are needed.

2.12.3.2.2 Proprietary Data

It is desirable that Proprietary data stored in an IS be encrypted using NIST-certified cryptography.

2.12.3.2.3 Sensitive Data

Sensitive data stored in an IS should be encrypted using NIST-certified cryptography.

2.12.3.3 Stored Data – Special Consideration for Backups

In many cases, Proprietary or Sensitive unencrypted data is stored in an IS and the authentication and access features of the IS are used to ensure the integrity and confidentiality of the data. When these systems are backed up, unencrypted Sensitive data may be created on backup tapes. Although it is preferable that this data also be encrypted, this may not be immediately realizable.

In this case, the backup procedures and on-site tape handling and storage must be adequate to ensure safeguarding of the data. Physical security and access procedures are part of the data security mechanisms.

If off-site storage of backups is maintained, the transportation of tapes and the off-site storage facility must also be adequately protected.

2.12.3.4 Wireless

All data transmitted wirelessly must be encrypted using NIST FIPS140-validated cryptography.

2.12.4 Summary of Data Protection Requirements

Table 1 summarizes the safeguard requirements when data is delivered to an external party.

Data	Storage	Encryption	External Party	FIPS140-2
Public	All	None	None	Not applicable
Proprietary	All	Required	NDA or MOA	Desired
Sensitive	Floppy disk	Required	MOA	Required
Sensitive	CD/DVD-ROM	Required	MOA	Required
Sensitive	Removable HDD	Required	MOA	Required
Sensitive	Thumb drive	Required	MOA	Required
Sensitive	Magnetic tape	Required	MOA	Required

Table 1. Data for Distribution - Protection Requirements.

Table 2 summarizes the data protection requirements for data stored in an IS.

Data	Storage	Encryption	FIPS140-2
Public	All	None	Not applicable
Proprietary	All	Desired	Desired
Sensitive	Floppy disk	Required	Required
Sensitive	CD/DVD-ROM	Required	Required
Sensitive	Removable HDD	Required	Required
Sensitive	Thumb drive	Required	Required
Sensitive	Magnetic tape	Required	Required
Sensitive	Laptop	Required	Required
Sensitive	Database	Required	Required
Sensitive	Desktop, Server (internal)	Required	Required
Sensitive	Desktop, Server (external inc. DMZ)	Required	Required

Table 2. Stored Data - Protection Requirements.

2.12.5 Waivers

A waiver from this policy may be requested for specific cases. The request should list:

1) why encryption isn't feasible;
2) what other protection mechanisms will be used to ensure confidentiality; and
3) what actions are being taken to achieve compliancy with this policy.

Waivers will only be granted for a maximum period of 12 months.

2.12.6 Breach of Policy and Enforcement

A breach of this policy could have severe consequences to DMDC and its ability to provide services. Violation of this policy may result in disciplinary action at the discretion of DMDC senior management. Severe, deliberate, or repeated breaches of the policy may be considered grounds for dismissal; or in the case of a DMDC contractor, termination of their contracted services. All employees and contractors are bound by these policies and are responsible for their strict enforcement.

POLICY 2.13 – Certification and Accreditation (C&A)

2.13 Policy Statement

All DMDC systems and applications must be accredited by the DAA and have an Authority to Operate (ATO), Interim Authority to Operate (IATO), or Interim Authority to Test (IATT) before being placed into production.

Systems must have security controls tested at least annually and be reaccredited every three years or whenever there is a major change to the system.

2.13.1 Scope

This policy applies to all systems that are owned, operated, or created by DMDC.

2.13.2 Rationale

DOD Directives and Instructions require that all systems are operated with IA in mind and that they have sufficient security controls built in. This policy represents the DMDC implementation of the accreditation requirements specified in:

- DODD 8500.1 Information Assurance (IA),
- DODI 8500.2 Information Assurance (IA) Implementation and,
- DOD 8510.01 Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) Instruction.

2.13.3 Policy Implementation

2.13.3.1 Overview

Security at DMDC is managed by the Chief Information Officer (CIO) via the DMDC Information Systems Security Group (DISSG) as a Life-Cycle process, beginning at project initiation. The DMDC security process is consistent with DIACAP per DOD 8510.01.

DISSG works with the Project Team to develop the specific security requirements. Beginning with business and security systems analysis, this process contains four major steps in building a security plan. Key management personnel work with stakeholders to define security requirements and relevant documentation, then verify, test, validate, certify, accredit, monitor and maintain them throughout the life-cycle of the application. Security evaluation is continuous throughout this process.

2.13.3.2 Security Process Operating Rules

The DMDC Security Process operates under the following rules:

1. The PM initiates the Security Process by registering a project with DISSG.
2. DISSG and the PM identify the Security Team comprised of the DAA, the PM, the Certifying Authority (CA) and stakeholders.
3. DISSG represents the DAA and leads the Security Team.
4. The Security Team develops the security plan for the project.
5. The PM shall allocate funding and resources for security evaluations based on
6. The Security Team must interface with the all functional groups throughout the entire life-cycle process – including project planning, design, documentation, development, testing, quality assurance, implementation, and operation.
7. At various points throughout the project, the Security Team will be temporarily augmented by experts for specialized technologies – e.g., smartcard, embedded chip vulnerabilities, specific biometrics, and cryptographic operations. The Security Team selects Subject Matter Experts wherever available (e.g., NSA, Sandia, Mitre, Los Alamos, and Xacta).
8. End-to-end testing will be done using on-site test facilities.
9. Security services provider agreements must be flexible enough to accommodate operational scheduling constraints or the security service provider will be reconsidered.
10. Schedule slippage shall not affect the amount of time allocated for security evaluations.
11. Security-related documents shall be shared on a need-to-know basis only. The final determination on the release of security information will be made by the Information Assurance Manager (IAM).
12. If security recommendations cannot be completed by the scheduled dates, they will be addressed on a risk-severity basis as they become available.
13. All project documents and security documents shall be placed under configuration control.

2.13.3.3 C&A Required Documentation

For any system, the CDP is the master security document. The CDP is generated by DISSG as part of the certification and accreditation; however it may include documents generated by other groups, e.g. Concept of Operations. Also, much of the information in the CDP is typically derived from other documents, such as functional requirements from design documents.

The three groups that generate security documents for DMDC are:

- Project Manager (PM)
- DMDC Information Systems Security Group (DISSG)

- Systems Integration and Technical Support Division (SITSD)

Also, the Certifying Authority (CA) provides input and review of the documents, and in some cases may even provided the first draft.

Many of the documents are actually developed collaboratively by two or more of the groups.

The following tables list the security documentation and the originator for each.

Document	Notes
Project Plan	
Design Documents	Specific design documents will vary by project and the development methodology selected. Design documents include technical requirements, architecture, and software development life cycle.
Concept of Operations (CONOPS)	
Security Concept of Operations (SCONOPS)	
Disaster Recovery Plan	
Secure Facility User's Guide	As needed.
Trusted Facility Manual	As needed.

Table 1. Documents generated by PM.

Document	Notes
CDP	Derives information from the PM project documents and includes: Mission Needs Statement System Boundary MAC Class Functional & Technical Requirements Security Requirements (and SRTM) System Architecture Interface Specification Threat Analysis CONOPS SCONOPS SFUG TFM Life-Cycle Plan Configuration Management Plan COOP/DRP Minimal Security Checklist Security Testing Plans and Reports
Interim Authority To Operate (IATO)	Signed by DAA
Authority To Operate (ATO)	Signed by DAA
System Architecture Analysis	This set of documents supports the CDP and may be incorporated into the CDP. For all but the most basic systems, testing is performed by an independent agent. DISSG is responsible for the generation of these documents, but it is done in coordination with the CA and with the aid of independent testers and evaluators.
Security Test Plans and Procedures	
Software, Hardware and Firmware Analysis	
Network Compliance Report	
Integrated Products Analysis	
Life Cycle Management Analysis	
Vulnerability Assessment	
Initial Certification Analysis	
Penetration Testing Analysis	
Security Test and Evaluation	
Penetration Testing Analysis	

Document	Notes
COMSEC Analysis	
Systems Management Analysis	
Site Accreditation Survey Analysis	
Contingency Plan Analysis	
Risk Management Analysis	

Table 2. Documents generated by DISSG.

Document	Notes
Life-Cycle Plan	SITSD is responsible for enterprise plans for Life-Cycle, COOP, and DRP. Similar plans for specific system must be integrated with the enterprise plans. SITSD does this in coordination with the PM and DISSG.
Continuity of Operations Plan (COOP)	
Disaster Recovery Plan (DRP)	

Table 3. Documents generated by SITSD.

2.13.3.4 C&A Required Documentation

Once a system has been accredited and is placed into operation, periodic tests and assessments must be performed in order to retain the accreditation. Table 4 lists the periodic requirements.

Originator	Document	Notes
DISSG	COMSEC Compliance Evaluation Contingency Plan Maintenance Configuration Management Review Risk Management Review Compliance Testing Results Compliance Validation Report	Periodic testing is performed in coordination with SITSD and the CA. Additionally, unannounced audits and testing may be performed.

Table 4. Continuous Review Reports generated by DISSG.

2.13.4 C&A Task Checklist

CERTIFICATION & ACCREDITATION CHECKLIST

GUIDANCE

Three entities interact to certify and maintain accreditation of a system. These are:

- Designated Approving Authority (DAA) has overall responsibility for accrediting an IT system, database, or application.
- Chief Information Officer (CIO) through the DMDC Information System Security Group (DISSG) has oversight responsibility for the C&A process as well as policies and guidance for security of DMDC systems, databases, and applications. DISSG represents the DAA throughout the C&A process.
- Project Office (PO) through a Project Manager (PM) is the division in charge of the project. The PM is typically the Division Chief or Deputy. The functional Information Assurance Officer (IAO) is assigned by DISSG to work with the project.

Certification & Accreditation Checklist			
Task Description		**Lead**	**Support**
Initiate C&A Project			
[ ]	Identify C&A need for specific project. This should occur at least 150 days prior to fielding to allow for resource scheduling.	PM	
[ ]	Obtain approval for C&A.	PM	DISSG
[ ]	Identify and provide funding.	PM	
Procure and Schedule C&A Resources			
[ ]	Develop Statement of Work (SOW) if necessary.	PM	DISSG
[ ]	Develop project plan and cost estimate.	DISSG	Xacta
[ ]	Review and approve project plan and cost estimate.	PM	DISSG
[ ]	Formally accept proposal and associated costs.	PM	

Certification & Accreditation Checklist

Task Description		Lead	Support
Manage Development of C&A			
[ ]	Kick-off meeting between DMDC and Xacta security subject matter experts (SME).	DISSG	
[ ]	Establish accreditation boundary.	PM	Xacta, DISSG
[ ]	Provide system documentation and information to Xacta SME.	PM	
[ ]	Review existing documentation and security policies	Xacta	
[ ]	Perform pre-certification testing and vulnerability analysis	Xacta	
[ ]	Prepare SRTM	Xacta	PM
[ ]	Prepare SRTM	Xacta	
[ ]	Prepare draft CDP	Xacta	
[ ]	Respond to Xacta SME requests for system information.	PM	DISSG
[ ]	Develop required documentation and processes as needed.	PM	
[ ]	Review status reports to track progress of C&A.	DISSG	
[ ]	Approve payment to Xacta contract for work accomplished.	DISSG	
[ ]	Assign roles and responsibilities for User Representative.	PM	
[ ]	Assign roles and responsibilities for IAO, Certification Authority, and Program Manager.	DISSG	
[ ]	Identify functional and technical POCs to work with Xacta SME.	PM	
[ ]	Accept and distribute draft deliverables within DMDC for review.	DISSG	
[ ]	Review draft deliverables, provide comments, and coordinate with DISSG.	PM	
Prepare Final C&A Documents			
[ ]	Accept and distribute final deliverable within DMDC for review.	DISSG	
[ ]	Review final deliverables, provide comments, and coordinate	DISSG	

Certification & Accreditation Checklist

Task Description		Lead	Support
	with Xacta.		
[ ]	Create Plan of Action & Milestones (POA&M) to address vulnerabilities resulting from test failures.	PM	DISSG
[ ]	Review C&A activity results and make accreditation recommendation to the Certifying Authority.	DISSG	
[ ]	Review C&A activity results and make accreditation recommendation to the DAA and acquire final determination.	DISSG	
[ ]	Distribute final C&A activity results and determination within DMDC, storing copies in DMDC central files.	DISSG	
[ ]	Distribute final C&A documentation to user community as required.	PM	
	Provide Oversight for System Security Posture		
[ ]	Determine how and when to mitigate identified risks. Decisions are documented on a POA&M that becomes part of the CDP, APPENDIX Q.	PM	DISSG
[ ]	Serve as DMDC POC for Service and Agency inquiries and direct to appropriate DMDC POC	PM	
[ ]	Distribute C&A documentation as needed, once need-to-know and appropriate clearance levels have been verified.	PM	
[ ]	Serve as POC for NSA assessments.	PM	DISSG
[ ]	Verify that programs, procedures, and policies outlined in the CDP are consistent with DMDC policy.	DISSG	PM
	Maintain C&A Documentation		
[ ]	Maintain a library of original CDP documents for DMDC.	DISSG	
[ ]	Establish configuration management procedures for C&A documentation in the DMDC central files.	DISSG	
[ ]	Manage and track C&A document configuration.	DISSG	
[ ]	Approve or reject requests for C&A initiatives, new or out-of-cycle.	DISSG	PM
[ ]	Document system changes and report significant changes to DISSG to facilitate the current state of CDPs.	PM	

Certification & Accreditation Checklist

Task Description		**Lead**	**Support**
[ ]	Review system changes to determine action required (documentation update only, retest and document, or full C&A).	DISSG	PM
[ ]	Update existing C&A documentation as needed.	DISSG	
[ ]	Review and approve updates to documentation.	DISSG	
[ ]	Distribute updates to user community.	PM	
[ ]	Verify that procedures and policies outlined in the CDP certification document are being supported and maintained.	DISSG	

2.13.5 Additional Information

The C&A process is a component of a larger process that fits within the DMDC Security Architecture. For a more detailed description, refer to the *DMDC Security Management Process* prepared by DISSG.

POLICY 2.14 – Access Policy

2.14 Policy Statement

Access to DMDC facilities, systems, or information will be granted solely to personnel who are cleared at the appropriate level and have a justifiable need. Access control procedures will operate on the principle of least privilege and must provide safeguards through appropriate identification, authentication, authorization and encryption techniques.

2.14.1 Scope

This policy applies to all persons that are granted network accounts or have been authorized to use DMDC information resources.

2.14.2 Rationale

The threat landscape to DMDC networks and information systems is constantly changing. The increasing capabilities of information systems and mobile devices create significant risk to DMDC resources. Control of access to all DMDC resources must be maintained and access reviewed on a regular basis to mitigate the associated risks posed by these evolving threats.

2.14.3 Policy Implementation

2.14.3.1 Network Access

All users requiring access to DMDC network resources must submit a Change Request with Division Chief approval that specifies their requirements. All outside users must specify in writing which DMDC resources they wish to access. All outside users must have a DMDC sponsor and must conform to the ADP Security Policy, including the Password Policy. Access to DMDC network resources will be for a limited duration, which will be specified by the Change Control Board. Per DOD regulations, all users who access DMDC network resources must pass a background investigation, commonly known as vetting, and receive an ADP rating commensurate with their requested access level.

2.14.3.2 Local Access

Local accounts to DMDC systems are not allowed except for users requiring local access to their portable devices or laptops. Local accounts for all other systems are only granted by exception and any requests for local accounts must follow the Policy Exception Procedures.

2.14.3.3 Remote Access

Remote access is defined as the process of accessing DMDC network and information resources from networks that are beyond DMDC's immediate control. Need for remote access will be determined and preapproved by the user's Division Chief. A change request must be submitted and approved prior to the user being granted remote access. Remote access will be conducted from Government Furnished Equipment (GFE) that is configured according to current DOD security requirements. Remote access from personal or non-GFE equipment is not allowed.

Remote access that consists of a user establishing a VPN connection to the DMDC enterprise network and opening a session with a DMDC terminal server is considered to be a form of remote display and input, not remote access per se. In this case, all processing is actually performed on the terminal server and the remote device is merely used for display or input. Non-GFE and personal equipment may be used for this purpose. Access to network resources other than via a terminal server is not allowed. Local resources, including internal and external drives, will not be allowed to attach through the terminal server session. The list of remote access users will be reviewed at least annually to determine current need. Accounts of remote access users who have been dormant for over 180 days will be deactivated. Exceptions to the remote access policy must be authorized and approved in writing according to the Policy Exception Request Procedures.

2.14.3.4 Privileged Access

Privileged access to systems is granted on a per user basis and must be authorized by the user's Division Chief. Privileged accounts, including administrative accounts, must be unique for each user and will not be shared. All users requiring privileged access must be vetted at the appropriate level prior to access being granted and complete advanced Security Awareness training.

POLICY 2.15 – Incident Response Policy

2.15 Policy Statement

All employees should be vigilant for security breaches. As soon as employees become aware of an incident, they should report it to their Supervisors and to DISSG. DISSG will manage, document, and log the investigation per the incident response process.

Authority

The DOD Critical Infrastructure Protection (CIP) mission is to ensure that the critical infrastructure assets on which the DOD depends are available when they are needed. In order to accomplish this mission, DOD has recently released guidance to facilitate compliance within the DOD IT Global Information Grid (GIG). DOD Instruction 8500.1 and 8500.2 invoke the requirement for DOD Information Technology assets to define and document an Incident Response (IR) Policy, and an associated Standard Operating Procedure (SOP). Accordingly, Defense Manpower Data Center (DMDC) policy states that all IT assets under the purview of the DMDC Designated Approval Authority (DAA), shall follow the policy outlined in this section.

Policy

- Once an employee is cognizant of an incident, he/she shall contact both the *DMDC Information System Security Group (DISSG)* representative, as well as the immediate local supervisor, to evaluate the possible incident. In no case shall just one entity, either the Supervisor or the DISSG make a binding determination without the other having participated. This dual control of the decision making process will guarantee that an impartial and informed evaluation has transpired.

- The DISSG shall always be informed either first or in conjunction with the functional managers. In no case shall there be remedial actions or determinations pursued until the DISSG has been notified and the incident has been duly examined and logged. Once notified, the DISSG will work in conjunction with the application senior managers and other available resources (e.g. Security Subject Matter Experts) to determine a viable and productive course of action.

- The DISSG, having oversight of DMDC's security assets and resources, shall provide guidance and security resources in a manner that best suits organizational security needs. The organizational security needs shall be determined by senior management, in conjunction with recommendations and consultation by Security Subject Matter Experts (SME) and DISSG.

- The DISSG will perform whatever investigation and information gathering is necessary to determine the cause and scope of the incident.

- While the DMDC policy is delineated in this document, documented Standard Operating Procedures (SOP) shall be maintained locally which clearly define the roles and responsibilities of individual employees, thus clearly establishing procedural mechanisms to support this Security Policy.

What Constitutes an Incident

An incident is the act of violating an explicit or implied security policy. DOD Information Technology (IT) Security Policy is detailed in DOD 8500.1 and implemented in DOD 8500.2. DMDC local Policy is located on the iWeb at the following URL, http://iweb/common/policies/ADP_Security_Policy.pdf.

Possible incidents may include, but are not limited to:

Possible Incidents
Attempts (either failed or successful) to gain unauthorized access to a system or its data
Unwanted disruption or denial of service
The unauthorized use of a system for the processing or storage of data
Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent

You are encouraged to report any activities that you feel meet these incident criteria to the DISSG, and your supervisor. It is our policy to keep any information specific to your systems confidential.

DISSG Contact Information

NAME	Phone	E-mail
Chris Grijalva (CIO)	831-583-2400	Christian.Grijalva@osd.pentagon.mil
Andrew Kennedy (IAM)	831-583-4123	Andrew.Kennedy@osd.pentagon.mil
Rikki Welsh (IAO/Security SME)	831-583-2400	Rikki.Welsh.ctr@osd.pentagon.mil
Regina Rogers (IAO)	831-583-2400	Regina.Rogers@osd.pentagon.mil

Claire LaVelle (IAO)	831-583-2400	Claire.LaVelle@osd.pentagon.mil

Process Guidance

These are the basic steps an employee should follow when he/she believes there is a security incident or compromise:

- Respond quickly. Alert both the DISSG and your manager. Traces are often impossible if too much time is wasted before alerting law enforcement or your own incident response team. Quick technical expertise is crucial in preventing further damage and protecting potential evidence.
- If unsure of what actions to take, DO NOT stop system processes, or tamper with files. This may destroy traces of intrusion.
- Follow organizational policies/procedures by documenting the information in the list below, to the best of your ability.
    - The date that the alleged incident was noticed
    - The time that the incident was noticed (including time zone data), and approximately how long it appeared to last
    - The name of the system being compromised
    - Location of the system that was the focus of the incident
    - The contact information of the person reporting the incident
    - The type of system compromised (e.g., a Web server, database server, e-mail server, network, or application), if known
    - Operating system and IP address of the system being attacked, if known
    - Description of the incident: as detailed a description of the incident as possible
    - Implications of the incident: the adverse effects on the company as a result of the attack
- Use the telephone to communicate. Attacker(s) may be capable of monitoring email traffic.
- Consider activating Caller Identification on incoming lines. This information may help in leading to the identification of source/route of intrusion.
- Pre-establish contacts that will help in a quick response effort.
- Make copies of files an intruder may have altered or left. If you have the technical expertise to copy files this action will assist investigators as to when and how the intrusion may have occurred.
- Identify a primary point of contact within DISSG to handle potential evidence. Establish chain-of-custody of evidence. Potential hardware/software evidence that is not properly controlled may loose its value.
- Do not contact the suspected perpetrator.

The DISSG in conjunction with management will decide on the optimum course of action for the specific investigation. Once it has been determined by the DISSG that an incident has occurred, a plan of action will be put into effect using either the ‘Protect & Forget” method or the “Apprehend & Prosecute” method. In no case is the employee who discovers the incident to take these measures. These procedures are reserved for the DISSG and mangers to pursue.

Either/both methodologies are defined in the next two sections.

The “Protect and Forget” Philosophy

Determine if event is a real incident

This is one of the most important aspects of handling any incident. The team must know if this is truly a computer security incident, as opposed to a user error or a system configuration error.

If so, terminate the current intrusion

This is the key part of “protect and forget.” The team must stop any further damage from being done to the system, or to information that the attacker takes off the system. Because it does not matter if the intruder knows that he or she was discovered, the team can just kill the session.

Discover how access was obtained and how many systems were compromised

The team needs to know how the person gained access to the system, as well as where they went while they had access. This reveals the vulnerabilities that need fixing and how many systems must be restored back to their pre-incident configuration. The team must also determine approximately when the first intrusion was made, to determine how far back to go, in order to obtain an uncompromised system backup.

Restore compromised systems back to the pre-incident configuration

This can be done from an uncompromised backup tape. However, all transactions that were performed after that backup was performed will be lost, and will need to be redone.

Secure the method of unauthorized access by the intruder on all systems

This means fixing the system vulnerability that was used to gain access. The corrections and fixes might entail turning off services that are not required by the system to operate and function, installing necessary software patches, or changing user passwords and enforcing good password practices.

Document steps taken to deal with the incident

Someone should take notes during the entire incident, documenting every step taken to combat it. The notes should include what was done, the exact time that it was done (including time zone information), who performed each step, and who witnessed the step. At the end of the incident, these notes should be collected and formalized into an after-action report.

Develop lessons learned

The after-action report should be reviewed by both the CIRT and the IT security program manager, giving rise to ideas for improvement such as modifying system security and configuration guidelines, improving user security awareness, modifying IT security policies and procedures, or modifying security incident response procedures.

Brief upper management on the aftermath of the incident

In the military, this is called an after-mission debriefing. Here, the IT DISSG and the cognizant operational manager should discuss the incident with upper management, in terms of what occurred, what was done to combat the incident, the results of the incident, and what must be done to prevent similar events from re-occurring. Although upper management must be kept informed of what is happening during the entire incident, it is at the end that they must be told the entire story.

The "Apprehend and Prosecute" Philosophy shall follow these procedures

Determine if the event is a real incident

This is one of the most important portions of handling the incident. The team must know if this is truly a computer security incident, as opposed to a user or system configuration error.

If the event is an incident contact law enforcement

If management has decided that it wants to pursue and prosecute the attacker, the local Police or the Federal Bureau of Investigation (FBI) must be notified as soon as it is verified that the incident is real. In most cases, law enforcement agencies will not step in and take over the incident. However, they will work with the team, ensuring that its actions stay within the law and do not violate any individual rights. They will assist the team in properly documenting and storing evidence to protect the chain of custody that is necessary for evidence to be used in court.

Document each action taken, including the date and time that the action was taken and who was present

In cases where the organization wishes to prosecute the attacker, it is absolutely necessary to be extremely precise in recording what action was performed, when it was performed, and who saw it being performed. The reason is that these notes can be used as evidence at the trial, if it goes that far. All notes must be protected using the rules of evidence that the courts have stipulated.

Isolate the compromised systems from the network

This is done to protect the remainder of the network. The organization must try to remove the system from the main part of the network without killing the attacker's session, because the team is still trying to track down the individual and obtain additional evidence against him or her.

If the organization has the capability, it should entice the intruder into a safe system (i.e., a honey pot) that seemingly contains valuable data

This is generally known as a “honey pot.” By providing the attacker with an area to play in that appears to have extremely vital information, he or she remains in this system for a while, giving the team time to trace the individual back home. There has been much discussion in security-focused mail lists 1 regarding honey pots. The general consensus is that they are too dangerous in most cases because they are difficult to configure in a secure manner. However, if the organization wishes to use one, it must be in place prior to the intrusion. Also, the login banner must indicate that people who access the site consent to monitoring.

Discover the identity of the intruder while documenting his or her activity

This is one of the reasons to bring in law enforcement early on. In most cases, attackers will not be attacking the system from their personal PCs or workstations. Instead, they will have compromised multiple sites and will use them as the conduit for their attack against the system. Some of these sites may be in a different country, requiring the assistance of a federal law enforcement agency to perform some of the tracing, such as the FBI in the United States, Scotland Yard in the United Kingdom, or Interpol. To be able to trace back through the various legs, the organization will also need the assistance of the various Internet service providers (ISPs) and telephone companies. Most ISPs and telephone companies will only provide assistance if are they served with a warrant for their records, and it is the law enforcement agencies that must usually obtain the warrants to perform searches. The international angle can make things even more difficult. In the meanwhile, the organization can document that the attack against the system is coming from “IP address A,” which would be owned by such IP address providers as ARIN, Network Solutions, RIPE, or APNIC, for example.

Discover how the intruder gained access to the compromised systems, and secure these access points on all uncompromised systems

The organization must know which vulnerability point the intruder used to gain access to the system. Once the vulnerability is known, it can be removed from the systems that have not been compromised but remain susceptible to that particular vulnerability. This prevents those systems from being compromised in the future by intruders using that hole in the system.

Terminate the current intrusion as soon as sufficient evidence has been collected, or when vital information or systems are endangered

The intruder’s session must be severed when the organization has collected sufficient evidence to use against him or her, or if the intruder is about to compromise a vital system or vital data.

Document the current state of compromised systems

The team must state whether the system was left in production, was taken offline and is being analyzed, is offline and ready to be restored to production, or is to be replaced by another system.

Restore the compromised systems back to the pre-incident configuration

The team must make sure that the systems' operating systems and application software are restored to the same condition they were in prior to the intrusion.

Secure the method of unauthorized access by the intruder on all compromised systems

The team must correct the vulnerability that was used to gain access to the systems. This could include installing the latest required patches for the system, upgrading to the latest version of the application software, changing user and system passwords, or some combination of these. When changing passwords, the new passwords must meet the password requirements stated in the organization's IT security policies, procedures, and guidelines. If these requirements are not strong enough, they should be modified.

Document the cost of handling the incident, and the time in man-hours

The cost can be used as part of the intruder's prosecution. If the intruder is convicted, it can then be used to help in sentencing.

Secure all logs, audits, notes, documentation, and any other evidence that was gathered during the incident, with appropriate identification marks, securing the "chain of custody" for future prosecution

Logs, audits, notes, and other documentation that is in paper form must be placed in thick envelopes that are securely taped. The envelopes must then be clearly marked, detailing what the envelope contains; who placed the items into the envelope, with the date and time this occurred; and the names of each person who then touched the envelopes, including the date and time. All logs, audits, notes, and other documentation stored on electronic media must be marked in a similar fashion. These markings must be permanent so that there is no question about the "chain of evidence." Also, at this time, a copy of these notes should be collected and formalized into an after-action report, and a copy of the latter should be placed with the rest of the evidence.

Develop lessons learned

The DISSG and the cognizant operational manager should review the after-action report, resulting in improvement ideas. These might include modifying system security and configuration guidelines, improving user security awareness, modifying IT security policies and procedures, or modifying security incident response procedures.

Brief upper management on the aftermath of the incident

The military calls this an after-mission debriefing. The DISSG and the cognizant operational manager hereby discuss the incident with upper management, in terms of what occurred, what was done to combat the incident, the results of the incident, and what must be done to prevent similar events from occurring. While upper management must be informed of what is going on during the entire incident, they must also be told the entire story at the end.

POLICY 2.16 – Security Training and Awareness

2.16 Policy Statement

All users of DMDC resources must complete security awareness refresher training at least annually. New users will not be given access to DMDC systems until they complete security awareness training, Privacy Act Training, and execute a User Agreement.

2.16.1 Implementation

DOD personnel, including contractors and task force members who are involved with management, use, or operation of any IT systems that handle sensitive information shall receive periodic training at least annually in security awareness, accepted security practices, and system rules of behavior. DOD personnel, including contractors and task force members with significant security responsibilities, shall receive specialized training specific to their security responsibilities annually. The level of training shall be commensurate with the individual's duties and responsibilities and is intended to promote a consistent understanding of the principles and concepts of IT systems security. Organizations shall have a means to track, by name and position, individuals who have received training, the type and name of the training, and the costs associated with the training.

a. DISSG shall establish an ISS training and awareness program.

b. Training may be presented in stages, for example, as more access is granted. In some cases, the training may be in the form of classroom instruction. In other cases, interactive computer sessions or well-written and understandable brochures may be sufficient, depending on the risk and magnitude of harm related to the subject matter.

c. Refresher awareness training frequency shall be determined by DISSG.

d. Each new user of a system in some sense introduces a risk to all other users. Therefore, each user should be versed in acceptable behavior – the rules of the system – before being allowed to use the system.

e. Training should be tailored to what a user needs to know to use the system securely, given the nature of that use, and how to get help in the event of difficulty with using or security of the system.

f. Access provided to members of the public should be constrained by controls in the applications through which access is allowed, and training should be within the context of those controls.

g. Additional awareness training will be provided when significant changes occur in ISS environments or procedures, or to employees who assume new positions or assignments dealing with information at a higher level of sensitivity.

h. Security awareness training should include the following topics, as appropriate.

1) Common IS threats, vulnerabilities, and risks.
2) Information accessibility, handling, labeling, and storage protection considerations.
3) Physical and environmental IS protection considerations.
4) IS data access controls and rules of behavior.
5) Procedures for disaster recovery and contingency operations plan.
6) ISS configuration management and control requirements.
7) IS-related security incident reporting requirements and procedures.

i. Specialized training is required for all individuals given access to an application, including members of the public. It should vary depending on the type of access allowed and the risk that access represents to the security of the application and information in it. This training will be in addition to that required for access to a support system. Such training may vary from a notification at the time of access (e.g., for members of the public using an information retrieval application) to formal training (e.g., for an employee that works with a high-risk application).

j. All personnel who design, develop, operate, or maintain sensitive IS will be provided security training appropriate to the level of risk they present to DMDC IS. The training shall address the types of security and internal control techniques that ought to be incorporated into IS development, operation, and maintenance.

k. All personnel in privileged roles, e.g. system administrators, shall receive specialized training appropriate to their roles.

POLICY 2.17 – Operational Security (OPSEC)

2.17 Policy Statement

Since an adversary can accumulate and correlate sensitive unclassified data from various sources to deduce useful and potentially damaging information, all users of DMDC resources need to be aware of the need for Operational Security (OPSEC).

OPSEC will be included in the annual Security Awareness and Training for all users.

2.17.1 Scope

This policy applies to all employees, contractors, consultants, temporaries, and other workers at DMDC, including those workers affiliated with third parties who access DMDC computer networks.

2.17.2 Rationale

The accumulation of elements of sensitive/unclassified information or data could damage national security by revealing classified information. The idea is that what you say may not be an OPSEC problem, but combined with what someone else says, it can reveal too much and could quite possibly risk lives. On the Internet, it could be what you say over the course of weeks or months being put together.

2.17.3 Policy Implementation

2.17.3.1 OPSEC Guidelines for Associate Conduct

All associates should practice operational security by adhering to the following guidelines:

- Do not conduct *any* work-related conversations in common areas, public places, while commuting, or over unsecured electronic circuits.
- Classified information may be discussed *only* in authorized spaces and with persons having a specific need-to-know and the proper security clearance. Likewise, unclassified information may require protection because it can often be compiled to reveal sensitive conclusions. Much of the information we use to conduct DMDC operations must be withheld from public release because of its sensitivity.
- Do not release or discuss official information except with authorized DMDC personnel with a valid need-to-know.
- Do not promote or identify yourself as a DMDC or government employee.
- Maintain a low profile and remain inconspicuous by ensuring that identification cards such as the CAC are hidden from plain view when not in Government facilities.

2.17.3.2 Third Party Disclosures

2.17.3.3 Preauthorization For Public Statements

All workers who will be delivering speeches, writing papers, or otherwise disclosing information about DMDC or its business shall obtain preauthorization from DISSG. Only individuals designated by the Director are authorized to be spokespersons for DMDC.

2.17.3.4 DMDC Non-Disclosure Agreements

Whenever DMDC needs to release sensitive information to an external party, the external party shall execute a Memorandum of Agreement (MOA) (see Data Security Policy). Information released to external parties shall be limited to the specific information necessary for the business relationship or project involved.

2.17.3.5 Third Party Non-Disclosure Agreements

In some instances, third parties will ask that DMDC associates execute a Non-Disclosure Agreement (NDA) before beginning discussions. Before signing, the Associate should forward the NDA to DISSG for review to ensure that no security policies are violated by execution of the agreement.

POLICY 2.18 – Information Operations Conditions (INFOCON)

2.18 Policy Statement

DMDC will comply with requirements for security posture based on updated cyber threat and INFOCON status.

2.18.1 Scope

This policy applies to all DMDC organizations and all systems owned or operated on behalf of DMDC.

2.18.2 Rationale

Increased connectivity and readily available low cost information technology make computer network attack (CNA) an attractive option for our adversaries. CNA includes attempts to disrupt, deny, degrade, or destroy information in our computers and networks. INFOCON levels focus on protective measures to be invoked when various conditions including attacks are detected. The INFOCON levels reflect increasing risk to information operations. To mitigate damage, more severe defense mechanisms must be employed at higher risk levels.

2.18.3 Policy Implementation

2.18.3.1 Description of INFOCON Levels

INFOCON levels indicate the relative degree of threat to DOD information technology systems. The overall INFOCON is established by the SecDef or the Chairman of the Joint Chiefs of Staff. However local situations may cause a higher local INFOCON to be declared.

There are five INFOCON levels defined as:

Level	Description	Criteria
Normal	Normal activity.	No significant activity.
Alpha	Increased risk of attack.	• Indications and warnings (I&W) indicate general threat. • Regional events are occurring which affect US interests and involve potential adversaries with suspected or known CNA capability. • Military operation, contingency, or exercise planned or ongoing requiring increased security of information systems. • Information system probes, scans or other activities detected indicating a pattern of surveillance.

Level	Description	Criteria
Bravo	Specific risk of attack.	• I&W indicate targeting of specific system, location, unit, or operation. • Major military operation or contingency, planned or ongoing. • Significant level of network probes, scans, or activities detected indicating a pattern of concentrated reconnaissance. • Network penetration or denial of service attempted with no impact to DOD operations.
Charlie	Limited attack.	• Intelligence attack assessment indicates a limited attack. • Information system attack detected with limited impact to DOD operations: (1) minimal success, successfully counteracted, (2) little data or systems compromised, (3) unit able to accomplish mission.
Delta	General attack.	• Successful information system attack detected with impact to DOD operations. • Widespread incidents that undermine ability to function effectively. • Significant risk of mission failure.

2.18.3.2 Declaring INFOCON Level

Current DOD INFOCON is declared by Secretary of Defense who may delegate declaration authority to JTF-CND. The Director of DMDC may change the local INFOCON; however, it must remain at least as high as the current DOD level. The Director may delegate this authority to the CIO or the Chief of the Systems and Technical Support Division.

When potential CNA events are observed, it is prudent to assume malicious intent until assessed otherwise. It’s not necessary that all criteria for an INFOCON be met before changing to that level. The decision to change INFOCON is tempered by the overall operational and security context at the time. For example, an intruder could gain unauthorized access and not cause damage to systems or data. This may warrant INFOCON ALPHA or even NORMAL during peacetime, but may warrant INFOCON CHARLIE during a crisis.

2.18.3.3 INFOCON Response Measures

DOD INFOCON measures focus on network-based protective measures.

Each level indicates an increase in the threat to DOD information technology systems. As the threat level increases, more stringent protective measures will be used.

The following table lists the defensive measures that should be in control for each threat level.

Level	Defensive Measures
Normal	• Maintain an inventory of all mission critical information systems, including applications and databases, and identify their operational importance. • Identify all points of access and their operational necessity. • Conduct normal security practices as described in the rest of this policy. • Conduct periodic internal security reviews and external vulnerability assessments. • Periodically review and test higher level INFOCON actions.
Alpha	In addition to all NORMAL measures: • Heighten awareness of all system users and administrators. • Increase level of auditing and review. • Conduct internal security review on critical systems. • Review higher level INFOCON actions and consider proactive execution. • Execute appropriate defensive tactics.
Bravo	In addition to all ALPHA measures: • Conduct immediate internal security review on all critical systems. • Check for existence of newly identified vulnerabilities (if any) and patch. • Disconnect unclassified dial-up connections not required for current operation. • Execute appropriate defensive tactics
Charlie	In addition to all BRAVO measures: • Conduct maximum level of auditing and review. • Disconnect non-mission-critical networks. • Reconfigure information systems to minimize access points and increase security. • Reroute mission-critical communications through unaffected systems. • Employ alternative modes of communication and disseminate new contact information. • Minimize external connections and consider limiting traffic to mission essential communication only • Execute appropriate defensive tactics
Delta	In addition to all CHARLIE measures: • Isolate compromised systems from rest of network. • Implement procedures for conducting operations in “stand-alone” mode or manually. • Execute procedures for ensuring graceful degradation of information systems. • Designate alternate information systems and disseminate new communication procedures internally and externally. • Execute applicable portions of COOP plan • Execute appropriate defensive tactics

2.18.3.4 Reporting

Local changes in INFOCON will be reported to the JTF-CND within 4 hours. Reporting of this change will be accompanied by an operational assessment of the situation when appropriate.

2.18.3.5 Sensitivity of Information

Generic defensive measures are unclassified.

Changes in INFOCON are OPSEC indicators and must be protected. Criteria and response measures are valuable to an adversary in assessing the effectiveness of a CNA and in analyzing DOD's response. INFOCON procedures shall not be posted in publicly accessible locations such as unclassified web pages or bulletin boards accessible to outsiders.

CNA intelligence assessments are classified SECRET or higher.

Operational impact of a successful information attack is classified SECRET or higher.

POLICY 2.19 – Portable Devices

2.19 Policy Statement

The use of portable devices must conform to all DOD and DMDC security policies as well as device-specific policies. Portable devices include laptops, PDAs, cell phones, thumb drives/USB drives, MP3 players, camcorders, digital cameras or any other device with storage, connectivity, or data capture capability. USB devices such as MP3 players, camcorders, or digital cameras are not to be attached to IS without DAA approval.

In general, use of personally owned devices other than cell phones is not allowed except in the conference area. In no case is it permissible to connect a personally owned device, including thumb drives, to DMDC equipment or networks without explicit authorization. Furthermore, no IS shall have its BIOS set to allow a boot from any USB device.

2.19.1 Scope

This policy applies to all persons entering or connecting to a DMDC managed facility.

2.19.2 Rationale

The increasing capability and connectivity of portable devices creates a significant risk to data security, e.g. PDAs with Internet connectivity can create backdoors into networks when they are connected to users desktops; cell phones with video cameras can facilitate undetected monitoring of computer screens or sensitive operations; or 4GB thumb drives can be used to easily transport entire databases without protection.

2.19.3 Policy Implementation

This policy distinguishes between use of portable devices in the DMDC Visitor Conference facilities and the rest of DMDC facilities. It also distinguishes between government-owned and personally-owned devices. Use of portable devices by visitors is restricted to the conference area unless explicitly authorized by DISSG. The general philosophy is: (1) the use of portable devices by visitors is prohibited except in the conference area; and (2) personally-owned devices are not allowed to be attached to government-owned equipment.

2.19.4 Use of Portable Devices in the Conference Center

2.19.4.1 General

In general, the use of portable devices in the conference area is permitted, subject to the following restrictions:

- Phones and messaging devices should have their ringers silenced.
- The use of cameras and other image capture devices (e.g., camera phones) is not permitted without explicit authorization.

- No device is to be connected to DMDC equipment or networks except by authorized DMDC personnel.
- Use of DMDC guest Internet access is for browser-based use only and must conform to the Appropriate Use policy outlined below. It is monitored.
- No network monitoring, sniffing, penetration, or hacking tools are allowed.

2.19.4.2 Cell Phones

Cell phones may be used in the conference area for placing and receiving calls or text messages. Cell phone ringers should be set to a silent mode so as not disturb sessions in progress. Other non-messaging use of phones, such as image capture, is not permitted without prior authorization.

Phones are not to be connected to DMDC equipment.

2.19.4.3 PDAs

PDAs may be used in the conference area in stand-alone mode for data retrieval and note-taking. PDAs may be used to access the Internet via their own wireless ISP or the DMDC-provided guest Internet access. PDAs with telephone capability may be used for placing and receiving calls or text messages. Ringers should be set to a silent mode so as not disturb sessions in progress. Image capture is not permitted without prior authorization.

PDAs are not to be connected to DMDC equipment.

2.19.4.4 Thumb Drives/ USB Devices

Thumb drives may only be used on the visitor's own equipment. If files need to be transferred from a thumb drive to DMDC equipment, e.g. a vendor's presentation, a DMDC associate must perform the transfer and must confirm that no executable files are included.

2.19.4.5 Laptops

Laptops may be used in the conference area in stand-alone mode for data retrieval and note-taking. Laptops may be used to access the Internet via their own wireless ISP or the DMDC-provided guest Internet access. Laptops with telephone capability may be used for placing and receiving calls or text messages. Ringers should be set to a silent mode so as not disturb sessions in progress. Image capture is not permitted without prior authorization.

Laptops are not to be connected to DMDC equipment.

2.19.4.6 Hybrid Devices

As hybrid devices emerge that combine the elements of several technologies, e.g. the PDA, it may not be obvious into which category a devices falls. In these cases, all policies related to any of the device's functions are in force. For example, a PDA with a USB interface for mass storage transfer would follow both the PDA and the thumb drive policies.

2.19.4.7 Internet Use

DMDC provides wireless guest Internet access in the conference area that enables connections to web sites, including SSL sites. Guests must adhere to the proscriptions on use in the DMDC Appropriate Use policy, namely:

- No use that impedes, interferes with, impairs, or otherwise causes harm to the activities of others, such as spamming, resource hogging, misusing mailing lists, chain letters, and hoaxes.
- No religious or political lobbying.
- No harassing or threatening use, including sexual, racial, religious, or ethnic.
- No use that may damage the integrity of DMDC or other IS, including attempts to defeat security, unauthorized access, network sniffing or monitoring, disguised use, distributing viruses.
- No illegal use such as promoting a pyramid scheme, child pornography, infringing copyrights, or making bomb threats.
- No gambling.
- No P2P file-sharing services.

Activity may be monitored and is subject to audit.

2.19.5 Use of Portable Devices by Visitors in non-conference areas

2.19.5.1 General

Except for cell phones without camera functions, visitor use of portable devices in DMDC facilities is prohibited without explicit authorization.

No device is to be connected to DMDC equipment or networks except by authorized DMDC personnel.

2.19.5.2 Cell Phones

Cell phones may be used for placing and receiving calls or text messages. Cell phone ringers should be set to a silent mode so as not to disturb workers. Other non-messaging use of phones, such as image capture or wireless connections, is not permitted without prior authorization

Phones are not to be connected, including via Bluetooth or infrared, to DMDC equipment.

2.19.5.3 PDAs

PDAs may be used in stand-alone mode for data retrieval and note-taking. PDAs may be used to access the Internet via their own wireless ISP. PDAs with telephone capability may be used for placing and receiving calls or text messages. Ringers should be set to a silent mode so as not disturb workers. Image capture is not permitted without prior authorization.

PDAs are not to be connected, including via Bluetooth or infrared, to DMDC equipment.

2.19.5.4 Thumb Drives/ USB Devices

Visitor use of thumb drives in non-conference areas is prohibited.

2.19.5.5 Laptops

Laptops may be used in stand-alone mode. Laptops may be used to access the Internet via their own wireless ISP. When authorized, laptops may be connected to the DMDC guest Internet (Visnet) by the Systems and Technical Support Division. Laptops are not to be connected to other DMDC equipment without explicit authorization.

2.19.5.6 Hybrid Devices

As hybrid devices emerge that combine the elements of several technologies, e.g. the PDA, it may not be obvious into which category a devices falls. In these cases, all policies related to any of the device's functions are in force. For example, a PDA with a USB interface for mass storage transfer would follow both the PDA and the thumb drive policies.

2.19.5.7 Internet Use

Guests accessing the Internet must adhere to the proscriptions on use in the DMDC Appropriate Use policy, namely:

- No use that impedes, interferes with, impairs, or otherwise causes harm to the activities of others, such as spamming, resource hogging, misusing mailing lists, chain letters, and hoaxes.
- No religious or political lobbying.
- No harassing or threatening use, including sexual, racial, religious, or ethnic.
- No use that may damage the integrity of DMDC or other IS, including attempts to defeat security, unauthorized access, network sniffing or monitoring, disguised use, distributing viruses.
- No illegal use such as promoting a pyramid scheme, child pornography, infringing copyrights, or making bomb threats.
- No gambling.
- No P2P file-sharing services.

Activity may be monitored and is subject to audit.

2.19.6 Use of Portable Devices in DMDC Facilities by DMDC Associates

2.19.6.1 General

In general, the use of portable devices is permitted subject to the following restrictions:

- Phones and messaging devices should have their ringers silenced.
- The use of cameras and other image capture devices (e.g., camera phones) is not permitted without explicit authorization.

- No device is to be connected to DMDC equipment or networks except by authorized DMDC personnel.

2.19.6.2 Cell Phones

Government-provided or personal cell phones may be used for placing and receiving calls or text messages. Cell phone ringers should be set to a silent mode when in common areas or shared space. Other non-messaging use of phones, such as image capture, is not permitted without prior authorization.

Personal phones are not to be connected to DMDC equipment.

2.19.6.3 PDAs

PDAs may be used in stand-alone mode for data retrieval and note-taking. PDAs may be used to access the Internet via their own wireless ISP or the DMDC-provided guest Internet access. PDAs with telephone capability may be used for placing and receiving calls or text messages. Ringers should be set to a silent mode when in common areas or shared space. Image capture is not permitted without prior authorization.

Personal PDAs are not to be connected to DMDC equipment.

2.19.6.4 Thumb Drives/ USB devices

Only Government-owned, IAO approved thumb drives/USB devices may be used. All USB devices must be powered off for at least 60 seconds prior to being connected to an IS. The USB device must remain without power for at least 60 seconds when disconnecting from one IS and connecting to a different IS to make sure enough time passes for all power to dissipate and the memory erased.

Proprietary or sensitive information on thumb drives must be encrypted. Personally owned thumb drives may not be connected to Government equipment without explicit authorization. Disguised thumb drives are banned from DMDC. Examples of disguised thumb drives include pens, watches, jewelry, etc. USB devices with persistent memory must be formatted in a manner to allow the application of Access Controls to files or data stored on the device. For devices used on a Windows system this would be an NTFS format.

2.19.6.5 Laptops

The use of laptops presents a significant risk to loss of data through theft. Government provided laptops must implement full hard disk encryption.

Personally-owned laptops may be used in stand-alone mode and, if authorized, may be connected to guest Internet access via Visnet. Personally-owned laptops are not to be connected to other DMDC equipment without explicit authorization.

2.19.6.6 Hybrid Devices

As hybrid devices emerge that combine the elements of several technologies, e.g. the PDA, it may not be obvious into which category a devices falls. In these cases, all policies related to any of the device's functions are in force. For example, a PDA with a USB interface for mass storage transfer would follow both the PDA and the thumb drive policies.

2.19.6.7 Internet Use

All Internet use must adhere to the proscriptions in the DMDC Appropriate Use policy, namely:

- No use that impedes, interferes with, impairs, or otherwise causes harm to the activities of others, such as spamming, resource hogging, misusing mailing lists, chain letters, and hoaxes.
- No religious or political lobbying.
- No harassing or threatening use, including sexual, racial, religious, or ethnic.
- No use that may damage the integrity of DMDC or other IS, including attempts to defeat security, unauthorized access, network sniffing or monitoring, disguised use, distributing viruses.
- No illegal use such as promoting a pyramid scheme, child pornography, infringing copyrights, or making bomb threats.
- No gambling.
- No P2P file-sharing services.

Activity may be monitored and is subject to audit.